

HANDBUCH

ekey net

Version 4.2 und höher

Eigenschaften des Dokumentes

VERSION	3
VERTRAULICHKEIT	PUBLIC
STATUS	Freigegeben
AUTOR	Thomas Reiter
PRÜFUNG	
VERTEILER	
ABLAGE	

Dokumentenhistorie

VERSION	DATUM	VERANTWORTLICH	ÄNDERUNGEN
1.0	24.03.2010	Picg	Erstversion
1.1	16.04.2010	Picg	Korrekturen und Ergänzungen
1.2	20.04.2010	Picg	Änderung der Produktnamen ekey net „private" -> „light" ekey net „print" -> „com"
1.3	27.6.2010	Brum	Betrieb FS ohne Lizenzaktivierung 30 Tage
1.4	15.8.2010	Brum	- Anzahl der Zeitfenstereinträge - ISO 14443 A/B rausnehmen - Ereignisumwandlung bei ekey net
1.5	2.12.2010	Reit	Korrekturen und Ergänzungen Neue Funktionen der V 4.0.6 ergänzt
1.6	25.5.2011	Reit	Neue Funktionen der V 4.1 ergänzt
1.7	05.9.2011	Reit	Änderungen Verbundsteuereinheiten
1.8	23.11.2011	Reit	Linzenzunterschiede überarbeitet
1.9	22.12.2011	Reit	SQL Table Typ geändert
2.0	09.01.2012	Reit	UDP Änderungen
2.1	02.02.2012	Reit	Wiegand Diagram

2.2	03.04.2012	Reit	Wiegand Diagram
2.3	14.05.2012	Reit	UDP Protokoll
2.4	10.07.2012	Reit	ekey net 4.1.8 Änderungen: Kapitel 6.6.7.2.2 Feirtagszuordnungen FREI 1-5 wurde entfernt Kapitel 8.1.1.5 Besondere MODI Für Zeitfenster – entfernt Alarmzonen entfernt und Screenshots geändert Kapitel 17 Alarmplan entfernt Lageplan entfernt Keine eigenen Photos mehr (User/Terminals)
2.5	2-11-2012	Reit	Änderungen Featureliste
3	10-1-2013	Reit	Info Verbund SE
4	14-11-2013	Reit	ekey net 4.2 Änderungen Wichtige Sonderseite bzgl. Änderungen ab SW 4.2 eingefügt

Berechtigung zu Änderungen

NAME	FIRMA	TELEFON	EMAIL
REIT	ekey biometric systems GmbH		



Änderungen mit ekey net Version 4.2

Im Zuge des Updates auf **ekey net Version 4.2** werden zahlreiche Änderungen eingeführt.
Es ergibt sich dadurch, dass je nach Softwarestand und Betriebsmodus verschiedene Punkte im Handbuch sowie Screenshoots nicht vorhanden sind bzw. leicht verändert erscheinen.

Betriebsmodus:
ekey net 4.2 kann in 2 verschiedenen Betriebsarten laufen, speziell für unsere neuen Fingerscanner wurde ein Modus geschaffen um eine noch bessere Erkennungsleistung zu erzielen.

Betriebsmodus (kann in den Optionen eingestellt werden)	
Classic	**Advanced**
Mischsysteme mit **Atmel und Authenthec** Sensoren **werden** weiterhin **unterstützt**. Sollten Sie ein Update durchführen startet die Software automatisch im Classic-Mode.	Es können **nur ekey net Fingerscanner mit Authenthec Sensoren** verwendet werden. **Bei einer Neuinstallation startet die Software automatisch im Advanced-Mode.**

Update von ekey net 4.x auf 4.2
Nachdem Update startet die Software im Classic Mode da bereits eine Installation erkannt wurde.

Verwenden Sie nur ekey net Fingerscanner mit Authenthec Sensoren,
haben Sie nun die Möglichkeit unter den Optionen auf „Advanced" umzuschalten.

Dadurch haben Sie eine bessere Ereknnungsleistung, ein neues Lernfingerkonzept, uvm.



Achtung:

- Alle User müssen danach neu eingelesen werden
- Alle Atmel Fingerscanner werden gelöscht
- Servermatching wird deaktiviert
- Fingerscannerfirmware ist im Programm Modulupdater upzudaten

Inhaltsverzeichnis

© 2010 – ekey biometric systems GmbH



DRUCKFEHLER, IRRTÜMER UND TECHNISCHE ÄNDERUNGEN VORBEHALTEN
VERSION: 1.7 vom 05.09.2011

1 Einleitung

1.1 Zweck desHandbuches

Das Handbuch soll dem Administrator und Anwender von ekey net schnelle und unkomplizierte Unterstützung bei der Inbetriebnahme und Wartung des Systems

ekey net

bieten und damit den ordentlichen und fehlerfreien Betrieb von ekey net gewährleisten. Weiters werden hier Empfehlungen zur Konfiguration von ekey net dargestellt, die in vielen Anwendungen erprobt wurden und damit hohe Betriebssicherheit des Systems gewährleisten.

1.2 Begriffsbestimmungen und Abkürzungen

ONLINE-Modus: ekey net FS und ekey net SE arbeiten im ONLINE-Modus, wenn eine Datenverbindung zum ekey net Terminalserverbesteht. Dabei sind alle Funktionen im Rahmen derLizenzversion uneingeschränkt verfügbar.

OFFLINE – Modus: ekey net FS und ekey net SE arbeiten im OFFLINE-Modus, wenn die Datenverbindung zum ekey net Terminalserver unterbrochen ist. Einige Funktionen sind dadurch nur eingeschränkt verfügbar.

SMTP Das **S**imple **M**ail **T**ransfer **P**rotocol (SMTP, zu deutsch etwa *Einfaches E-Mail-Sendeverfahren*) ist ein Protokoll der Internetprotokollfamilie, das zum Austausch von E-Mails in Computernetzen dient. Es wird dabei vorrangig zum Einspeisen und zum Weiterleiten von E-Mails verwendet

Terminal unter Terminals sind ekey net spezifische-Hardwarekomponenten(Geräte) zu verstehen.

Gerät im ekey net sind unter Gerätealle Hardwareeinheiten, wie

- ekey net FS
- ekey net SE
- ekey net SE REG
- ekey net CV LAN
- ekey CV WIEG

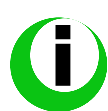
zu verstehen.

Anschluss im ekey net ist unter Anschluss ein Schaltelement (Aktor) zu verstehen. z.B. gibt es bei der ekey net 3 SE AP3 Schaltelemente (=Relais). Diese werden im ekey net als Anschluss1, Anschluss2 und Anschluss3 bezeichnet.

RFID-Terminals sind eine Teilmenge der Terminals. Diese RFID-Terminals sind ekey net (S,M,L) FS AP mit einem implementierten RFID-Empfänger/Leser, die eine Erkennung von Finger und/oder Karte ermöglichen.



Terminalgruppe: im ekey net werden Terminals zu einzelnenTerminalgruppen zusammengefasst und organisiert. Die Terminalgruppe steht immer einem ekey net Terminalserver vor, hierarchisch darunter liegen dann die ekey net CV LAN und unter diesem werden dann, hierarchisch gesehen, die Terminals(ekey net FS, ekey net SE,…)platziert.



Während der ekey net Terminalserver eine unbegrenzte Anzahl von ekey net CV LANverwaltet, kann der ekey net CV LAN maximal 8 Terminals verwalten.
Details über technische Grenzen entnehmen Sie bitte dem Dokumant „ekey net Spezifikation“.

Enrol(l)ment: Aufnahme der biometrischen Merkmale (Fingerprint) einer Person.

Aktion: im ekey net wird eine „Aktion“ definiert, als eine Handlung die ekey net anGeräten (Aktoren) ausführt. z.B. Impuls Relais 1. Einer Aktion geht immer ein Ereignis voraus.

Ereignis: Ein „Ereignis“ ist im ekey net eine Eingabe ins System.Dieser Eingabe vorausgehend ist praktisch immer ein Fingerzug über den Sensor. Diesem Fingerzug wird dann ein Ereignis zugeordnet: z.B. Mit FingerTüre öffnen

Update: beschreibt den Vorgang, bereits vorhandene Hard- und Software von ekey net auf einen neueren Stand zu bringen. Dies kann sowohl die ekey net Software, als auch die Firmware der Hardwarekomponenten betreffen. Ein Update wird also nur durchgeführt werden, wenn bereits eine Version von ekey net existiert.**Beispiel: Ein Update von ekey net 3.4 auf ekey net 4.0**

Upgrade: bezeichnet die Steigerung der Nützlichkeit oder Qualität von Hard- und Software. Oft ist dies mit einer neuen Version verbunden. **Beispiel: Ein Upgrade von ekey net 4.0 light auf ekey net 4.0 business**

Downgrade: gegenteiliger Vorgang zu Upgrade oder Update

Bereich: Innerhalb der Terminalstrukturvonekey net können Bereiche definiert werden. Dabei können als Bereichsgrenzen ekey net Terminalserver oder ekey net CV LAN gelten. Es besteht dann die Möglichkeit Aktionen auszulösen, die auf alle Geräte innerhalb dieser Bereichsgrenze wirken**.**

Schnittstelle: bezeichnet den datentechnischen Übergang zwischen einem elektronischen System zum anderen. Nur wenn die Definitionen der Schnittstelle auf beiden Seiten bekannt sind, können Informationen ausgetauscht werden.

Wiegand: Spezielle Datenschnittstelle – Bei Gerätebezeichnungen abgekürzt mit WIEG.

MS Windows-Dienst:

UDP: **User Datagram Protocol,** ist ein minimales, verbindungsloses Netzwerkprotokoll, das zur Transportschicht der Internetprotokollfamilie gehört. Aufgabe von UDP ist es, Daten, die über das Internet übertragen werden, der richtigen Anwendung zukommen zu lassen.

VPN **v**irtual **p**rivate**n**etwork



Network Time Protocol (NTP) ist ein Standard zur Synchronisierung von Uhrzeiten inComputersystemen über paketbasierte Kommunikationsnetze. NTP verwendet das verbindungslose Transportprotokoll UDP. Es wurde speziell entwickelt, um eine zuverlässige Zeitgabe über Netzwerke mit variabler Paketlaufzeit zu ermöglichen.

Unicode (Dt. etwa: "Einheitssschlüssel") ist ein alphanumerischer Zeichensatz, ein von der internationalen Standardisierungs-Organisation ISO genormtes System zur Kodierung von Textzeichen (Buchstaben, Silbenzeichen, Ideogrammen, Satzzeichen, Sonderzeichen, Ziffern). Unicode ist der Versuch, weltweit alle bekannten Textzeichen in einem Zeichensatz zusammenzufassen, also nicht nur die Buchstaben des lateinischen Alphabets, sondern etwa auch das griechische, kyrillische, arabische, hebräische, thailändische Alphabet und die verschiedenen japanischen (Katakana, Hiragana), chinesischen und koreanischen Schriften (Hangul). Außerdem können mathematische, kaufmännische und technische Sonderzeichen im Unicode kodiert werden.

ASCII: ist eine 7-Bit-Zeichenkodierung und bildet die US-Variante von ISO 646sowie die Grundlage für spätere mehr-bitige Zeichensätze und Kodierungen.

CSV: Das Dateiformat CSV beschreibt den Aufbau einer Textdatei zur Speicherung oder zum Austausch einfach strukturierter Daten. Die Dateiendung CSV ist eine Abkürzung für Comma-Separated Values (seltener Character Separated Values oder Colon Separated Values). Ein allgemeiner Standard für das Dateiformat CSV existiert nicht,jedoch wird es im RFC 4180 grundlegend beschrieben. Die zu verwendende Zeichenkodierung ist ebenso wenig festgelegt; 7-bit ASCII gilt weithin als der kleinste gemeinsame Nenner.

SQL: das Kürzel für *Structured Query Language*; ist eine Datenbanksprache zur Definition, Abfrage und Manipulation von Daten in relationalen Datenbanken. SQL ist von ANSI und ISO standardisiert und wird von fast allen gängigen Datenbanksystemen unterstützt. SQL umfasst die folgenden Datenbanksprachen: Data Manipulation Language, Data Definition Language, Data Control Language.

© 2010 – ekey biometric systems GmbH

1.3 Symbolbeschreibung

LIGHT Diese Symbol zeigt, dass die Funktion, bzw. Einstellung in der ekey net-Version „LIGHT" zur Verfügung steht.

COM Diese Symbol zeigt, dass die Funktion, bzw. Einstellung in der ekey net-Version „COM" zur Verfügung steht.

BUSINESS Diese Symbol zeigt, dass die Funktion, bzw. Einstellung in der ekey net-Version „BUSINESS" zur Verfügung steht.


ACHTUNG ! Dieses Symbol zeigt ihnen einen speziellen Hinweis den Sie bei der beschriebenen Funktion unbedingt beachten müssen.


Informationssymbol,Hier finden Sie Zusatzinformationen zu einer Funktion / einem Parameter.



Dieses Symbol zeigt ihnen, dass Sie eine Aktion unter keinen Umständen ausführen sollen. Meist müssen Sie um die Funktion auszuführen, vorher Einstellungen machen.

1.4 Zusammenhang mit anderen Dokumenten

ekey_net_4.0_spezifikation_de.pdf

2 Systemaufbau

ekey net verbindet mehrere verteilte biometrische Fingerprintleserund Aktoreinheiten (ekey net SE) zu einem leistungsfähigen Zutrittskontrollnetzwerk und ermöglicht eine komfortable Verwaltung von Benutzern, Terminals, Zeitfenstern und Kalendern direkt amPC (Server).

2.1 Architektur des Systems

BILD 1

Bild 1 zeigt einen möglichen Systemaufbau von <u>*ekeynet*</u>. Im Headoffice (Zentrale) ist der im System einmalig vorhandene <u>*ekeynet Masterserver*</u> platziert, dessen Aufgaben im Wesentlichen die Datenbankverwaltung und die Kommunikation zu den einzelnen <u>*ekey net Terminalserver*</u> sind.Die hierarchisch darunter angeordneten<u>*ekeynet Terminalserver*</u>sindfür die Kommunikation mit den einzelnen <u>*ekey net CV LAN*</u>zuständig und verwalten damit wiederum die hierarchisch darunter platzierten Gerätegruppen (Fingerscanner, SE). Ein <u>*ekey net CV LAN*</u> kann maximal 8 Geräte (Fingerscanner, SE) verwalten. Die Administration des Systems ekey net erfolgt mit der Anwendung <u>*ekey net Admin*</u>. „L“ Fingerscanner sind einzelnen CV-LAN`s zu betrieben. Weiters ist ein Mischbetrieb von „Atmel“ und „Authentec“ Fingerscannern am gleichen CV-LAN nicht möglich. Bei Verwendung von „L“ Fingerscannern ist nur 1 Fingerscanner pro CV LAN möglich, dies sollte auch bei der Betriebsart „Servermatching“ so gehandhabt werden.



Die Architektur des Systems erlaubt auch die Terminalinstallation in Filialen durch Kommunikation via VPN-Verbindungen. Dabei sind 2 Ausbaustufen möglich. Erstens mit einem eigenen *ekeynet Terminalserver* in der Filiale oder zweitens, ausschließlich die Anbindung über den *ekey net CV LAN*, der in kleinen Filialen die Terminalserver-Funktion eingeschränkt übernehmen kann.

Im System ist ausschließlich ein *ekey net Masterserver* vorhanden. e*keynet Terminalserver* und *ekeynet Admin* können grundsätzlich beliebig viele installiert werden. Allerdings gibt es hier von Betriebssystemseite Einschränkungen. So können Windows-Betriebssysteme, welche keine Serverbetriebssysteme sind, maximal 10 Terminalserver bzw. Terminalkommunikationen (hier sind auch andere Terminaldienste als *ekey net Terminalserver*, die eventuell am Masterserver-Rechner laufen, zu berücksichtigen) verwalten.
Physikalisch können *ekeynet Masterserver*, *ekeynet Terminalserver* und *ekey net Admin* auf einem Rechner betrieben werden, können aber auch getrennt auf Einzelrechner installiert werden. Wichtig ist nur, dass in diesem Fall auf jedem Rechner der *ekey Communicationserver*installiert und als Dienst aktiviert ist.



*Der Systemdienst **ekey Service Guard** überwacht alle ekey net Systemdienste und startet diese automatisch neu. Sollen ekey net Systemdienste zu Wartungszwecken gestoppt werden, müssen Sie **vorher den ekey Service Guard stoppen!***

Basis der Kommunikation ist Microsoft Message Queing (MSMQ). Der Datenaustausch zwischen den Serverdiensten bis hin zu ekey net CV LAN erfolgt über UDP – Datenpakete. Der Datenaustausch ist nicht transportgesichert!

2.2 Eingaben ins System

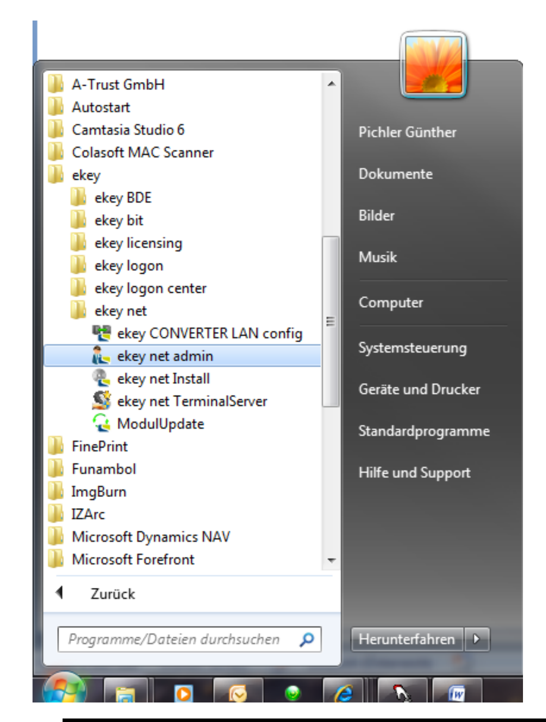
Eingaben in das System ekey net können über folgende Schnittstellen passieren:

- ekey net Admin
- ekey net FS
- ekey net SE (nur bei Versionen mit digitalen Eingängen)
- ekey net SDK(Softwareschnittstelle ekey net -> ist in diesem Handbuch nicht beschrieben).

2.2.1 ekey net Admin

Der*ekey net Admin* dient zur Konfiguration des Systems ekey net. Starten Sie den *ekey net Admin* aus dem Windows Programmverzeichnis. Der *ekey net Admin* wird im Kapitel 6.1 detailliert beschrieben.





2.2.2 ekey net FS



Über die ekey net FS erfolgt die Erfassung der Finger und damit die Eingabe der Benutzerdaten im laufenden Betrieb. Nach Erfassung eines Fingers an den ekey net FS, lösen diese definierte Ereignisse aus, die wiederum definiert (über den ekey net Admin zugewiesene) Aktionen an den Aktor-Einheiten (ekey net SE) nach sich ziehen.

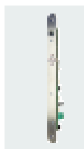
2.2.3 ekey bit und ekey net RFID Tischlesegerät



ekey bit ist ein Fingerscanner mit USB-Schnittstelle. Der Fingerprintleser wird im System ekey net zur Erfassung (Fingeraufnahme) der Benutzerfinger verwendet. Somit können die Benutzerfinger zentral beim Administrator eingelesen werden. Die am ekey bit erfassten Fingerprints werden dann entsprechend der Berechtigungsstruktur an die ekey net FS verteilt.

Ekey net RFID Tischlesegerät ist ein USB Desktop Lesegerät für RFID Karten. Somit können RFID-Cards dem User am PC-Arbeitsplatz zugwiesen werden.

2.2.4 ekey net SE

Eine Eingabe ins System bei ekey net über den Aktor ist nur bei

- ekey net SEIN (integra)
- ekey net SEmini
- ekey net 4 SE REG

möglich.
DieseGerätetypen stellen einen oder mehr digitale Eingängezur Verfügung, die z.B. für Türzustandsüberwachungen usw. verwendet werden können.
Siehe dazu Kapitel 4.2.3

3 Lizenzierung

3.1 Lizenzmodelle

ekey net ist mit verschiedenen Lizenzmodellen, die auch den Leistungsumfang des Systems definieren, verfügbar. Die Lizenzvarianten sind:

- LIGHT
- COM
- BUSINESS (ekey net 3.x entspricht der ekey net business – Variante)

In den folgenden Kapiteln zeigen ihnen diese Symbole

LIGHT	COM	BUSINESS

ob der Parameter / die Funktion im entsprechenden Lizenzmodell verfügbar ist.

Die Lizenzmodelle spiegeln einen eingeschränkten oder vollen Funktionsumfang wider und sollen für Sie als Kunde, die optimalen Leistungen für ihre Anwendung garantieren. Die Kosten für die entsprechenden Lizenzen variieren natürlich auch mit dem Lizenzmodell.

Grob kann gesagt werden:

Modell „LIGHT":	für Privatanwender (eingeschränkter Funktionsumfang)
Modell „COM":	für Druckeranwendungen und Zeiterfassung (eingeschränkter Funktionsumfang)
Modell „BUSINESS":	Vollversion (Die Version ekey net 3.X entspricht der business – Version)



Es ist nicht möglich Mischformen zu realisieren. Sie können nur das gesamte Systemekey net in einem Modell betreiben. Das heißt, wenn Sie einen Fingerscanner mit Lizenz „BUSINESS" erwerben, können Sie diesen nicht im ekey net als „LIGHT" –Variante betreiben!

3.2 Upgrade

ekey net lässt nur ein Upgrade von

- LIGHT ->BUSINESS
- COM ->BUSINESS

zu. Es ist nicht möglich, die Lizenzen von LIGHT auf COM zu ändern. Weiters ist auch ein Downgrade von BUSINESS auf LIGHT/COM nicht möglich.

© 2010 – ekey biometric systems GmbH



3.3 Unterschiede der Lizenzmodelle



Lizenzmodelle ekey net „Light“ und ekey net „Com“ sind erst ab Version 4.0 verfügbar. Für die Version ekey net 3.5 gilt das Lizenzmodell „BUSINESS“.

Funktionen im ekey net in Abhängigkeit des Lizenzmodells:

FUNKTION im ekey net	LIZENZMODELL		
	BUSINESS	LIGHT	COM*
Fingerscanner-Bauformen aufputz (AP), unterputz(UP), einbaubar (IN) und im Türgriff (FSB)	AP, UP, IN, FSB	AP, UP, IN, FSB	AP, UP, IN
Fingerscanner-Varianten (S = 40, M = 200, L = 2.000 Finger)	S, M, L	S, M	S, M, L
Anzahl der Zeitfenster	UNBEGRENZT	3	1
Benutzergruppen	UNBEGRENZT	1	UNBEGRENZT
Terminalgruppen	UNBEGRENZT	1	UNBEGRENZT
Anzahl Standorte per VPN	10		
Anzahl Terminalserver	10		
Verwaltbare Fingerscanner im System	80		
Verwaltbare Benutzer im System	4.000		
Zutritt	JA	JA	NEIN
Anzahl Einträge pro Zeitfenster	31	12	1
Anwesenheitsliste	JA	NEIN	NEIN
Kalender	UNBEGRENZT	1	KEIN
Easy-Mode	JA	JA	JA
Fingeraufnahme über USB-Fingerscanner und Fingerscanner vor Ort	JA	JA	JA
Portiermodus	JA	NEIN	NEIN
RFID	JA	JA	JA
WIEGAND	JA	NEIN	JA
Grundeinstellungen veränderbar	JA	NEIN (vordefiniert)	JA (eingeschränkt)
Kundenspezifische Gerätedefinition (Aktionen, Ereignissumwandlung)	JA	NEIN	NEIN
E-Mail Notification	JA	NEIN	NEIN

CSV Logging		JA	Nur positive	JA
ekey-Reporting		JA	NEIN	NEIN
ODBC(SQL) Logging		JA	NEIN	JA
HTML Logging		JA	NEIN	JA
UDP Logging		JA	JA	JA
Zeitsteuerung		JA	NEIN	NEIN
Zeitgesteuerte Wiedereintrittssperre (Min)		JA	JA	NEIN
Max. Anzahl der Relais die mit 1 Finger geschalten werden können		2	2	0
Handyöffnung mittels Einmal-PIN zur erhöhten Sicherheit		JA	JA	NEIN
Offlinefähigkeit		JA	JA	JA
Anzahl Relais 1 - 28		JA	NEIN	NEIN
Tagschaltung mit oder ohne Ersteintritt		JA	JA	NEIN
Bereichsschaltung(en)		JA	JA	NEIN
mehrsprachig		JA	JA	JA
Feiertagskalender		JA	JA	JA
* nur für Zeiterfassung oder Drucker				



3.4 Lizenzkey

Ab der Version 3.5 ist für den Betrieb von ekey net FS im Systemverbund ekey net ein Lizenz-Key notwendig.

Lizenzkeys brauchen Sie für

- die Neuinbetriebnahme von ekey net FS im ekey netab Version 3.5.
- das Update von ekey net 3.4 und ältere Versionen auf ekey net 4.0 für jeden Fingerscanner (hier erhalten Sie die Lizenzkeys kostenlos – **siehe Kapitel 5.3!)**
- Für das Upgrade von ekey net light (com) auf ekey net business
- das Downgrade von ekey net FS mit Firmwareversion 5.X.X.X auf Version 4.1.6.3 zum Betrieb in ekey net Systemen älter als 3.5

Bestellen Sie bei ekey entsprechende Lizenzen, so müssen Sie wissen, was Sie mit dieser Lizenz machen wollen (Upgrade, Downgrade, Neuinbetriebnahme) und Sie müssen die Anzahl der Fingerscanner wissen. Für jeden Fingerscanner müssen Sie eine Lizenz haben. Die Lizenzen können Sie in Paketen von 1- 30 Stk. erwerben.



Die Lizenzpakete sind nicht teilbar und sind mit dem ekey net Masterserver verbunden!

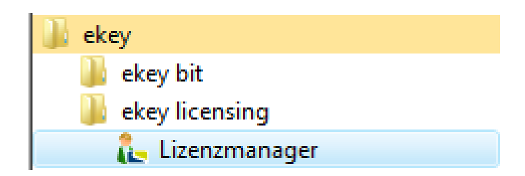
- ekey net business
- ekey net light
- ekey net com
- ekey net Upgrade
- ekey net Modul- Downgrade

3.5 LizenzManager (License Manager)

Der LizenzManager dient zur Verwaltung von Lizenzkeys für die ekey – Softwarekomponenten ekey net / ekey logon usw. Der LizenzManager wird automatisch auf dem Server/Rechner installiert, auf dem auch der ekey net Masterserver installiert wird. Im LizenzManager können Sie:

- Lizenzen Hinzufügen
- Lizenzen Online aktivieren
- Lizenzen Offline aktivieren
- Lizenzen löschen

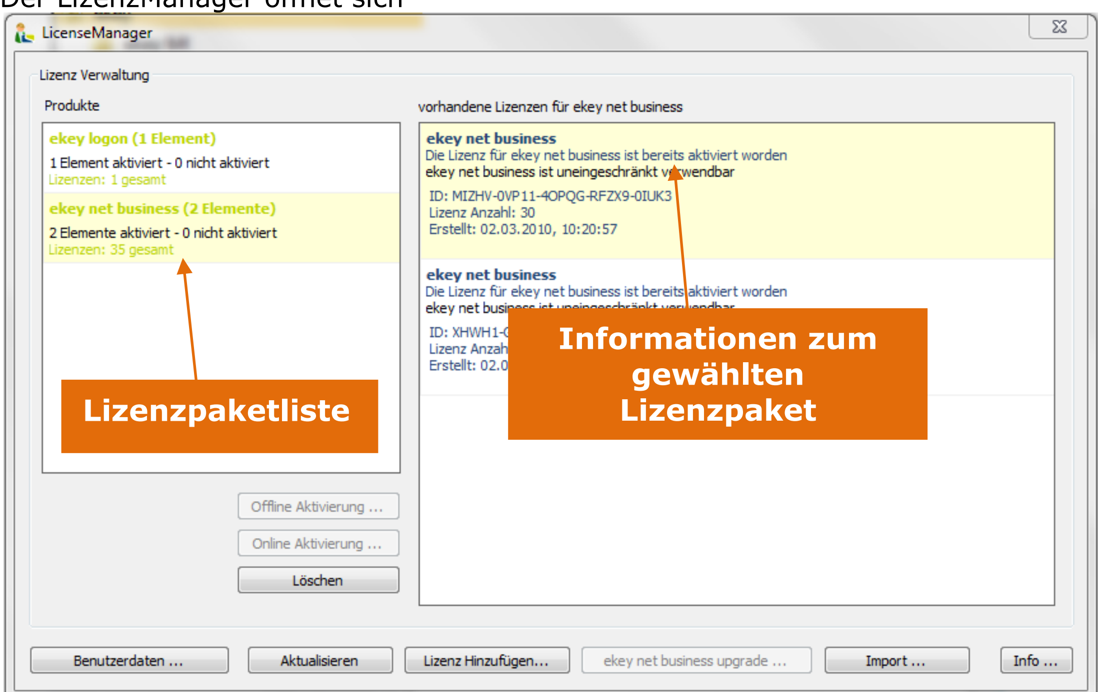
Starten Sie den LizenzManager im „Startmenü" -> „Programme"-> „ekey" mit einem Klick.





Lizenzbearbeitung (hinzufügen, aktivieren, importieren,...) inekey net ist immer auf dem PC/Server durchzuführen, auf dem auch der ekey net Masterserver installiert ist!!!

Der LizenzManager öffnet sich



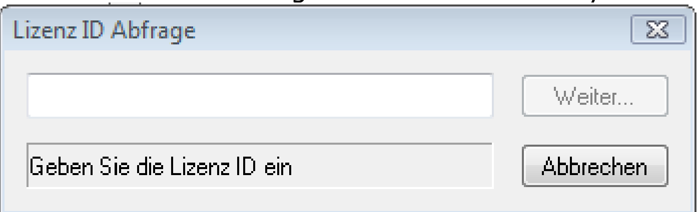
In der Lizenzpaketliste (Produkte) sind alle ekey eigenen Lizenzpakete gelistet. Wählen Sie dort mit einem Mausklick ein Paket aus, so sehen Sie im rechten Fenster Informationen zu dem Paket z.B.:

ekey net business
Die Lizenz für ekey net business ist bereits aktiviert worden
ekey net business ist uneingeschränkt verwendbar
ID: MIZHV-0VP11-4OPQG-RFZX9-0IUK3
Lizenz Anzahl: 30
Erstellt: 02.03.2010, 10:20:57



3.5.1 Lizenz Hinzufügen

Damit können Sie neue Lizenzen hinzufügen. Klicken Sie dazu auf den Button [Lizenz Hinzufügen...] und geben Sie die von ekey erhalten Lizenz ID ein. z.B.



3.5.2 Lizenz aktivieren

Lizenzen müssen, damit Sie auch wirksam werden und lizenzbasierende Geräte (z.B. ekey net FS) funktionieren, nach dem „Hinzufügen" aktiviert werden. Diese Aktivierung erfolgt entweder

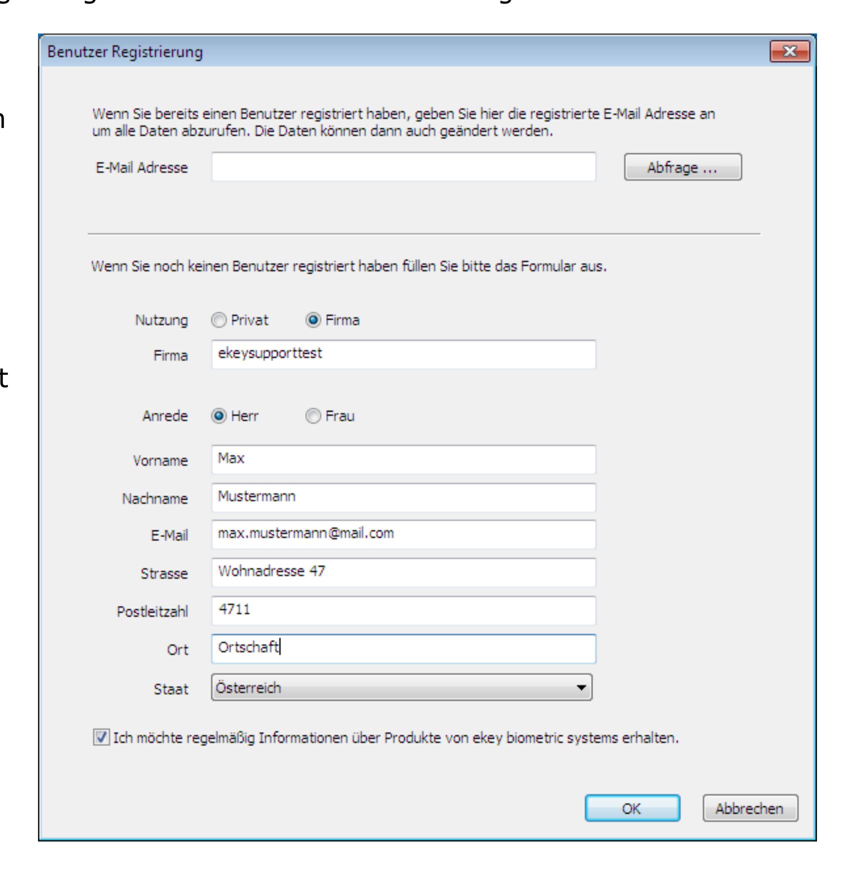
- **Online:** über das Internet ->Sie benötigen hier eine Internetverbindung am Server/Rechner
- **Offline:** per Email an ekey

Die Aktivierung bedeutet, dass Ihre Kunden- und Rechnerdaten an ekey übermittelt werden und eine Freischaltung der Lizenzen zurückübermittelt wird.

Wahlen Sie dazu in der Lizenzpaketliste das zu aktivierende Lizenzpaket ausund klicken Sie auf den jeweiligen Button für:

- [Offline Aktivierung ...] … Aktivierung erfolgt über Email-verkehr
- [Online Aktivierung ...] … Aktivierung erfolgt über eine Internetverbindung

Danach öffnet sich dieBenutzerregistrierung: Unabhängig von der Art des gewählten Aktivierungsmodus ist, sofern noch kein Benutzer registriert wurde, eine Benutzerregistrierung durchzuführen. Füllen Sie dazu alle Felder im Registrierungsformular aus.

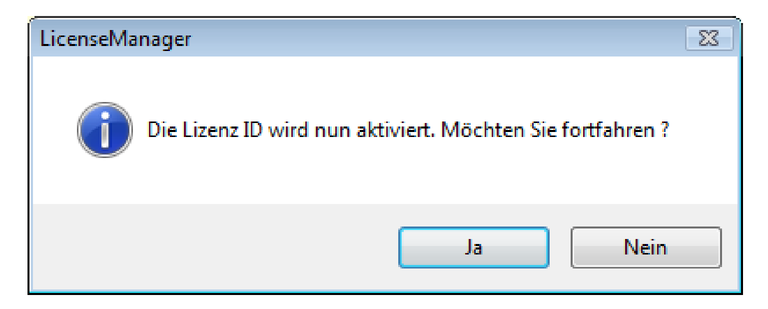


Erklärung zum Datenschutz: Um Ihnen gezielt Dienstleistungen und Support bieten zu können, ist die Angabe Ihrer Kontaktdaten notwendig. Wir versichern Ihnen, dass die von Ihnen angegebenen persönlichen Daten streng vertraulich und zweckbestimmt behandelt werden.
Es erfolgt keinerlei Weitergabe Ihrer persönlichen Daten an Dritte. Wir schützen die uns anvertrauten persönlichen Daten unter strikter Einhaltung der gesetzlichen Bestimmungen.

Wenn Sie schon registriert sind, brauchen Sie nur im 1. Feld ihre Emailadresse eingeben und aufAbfrage klicken. Ihre Daten werden dann über Internet abgefragt (nicht bei Offline-Registrierung).



Merken Sie sich unbedingt die Emailadresse, unter der Sie die Lizenz aktivieren. Die Lizenz kann nur mit der gleichen Emailadresse zwei weitere Male aktiviert werden!





Für die Aktivierung der Lizenzen haben Sie 30 Tage Zeit. Wenn die Aktivierung nicht erfolgt, so schaltet das System in den Offline-Modus und Sie können keine Konfigurationsänderungen durchführen.

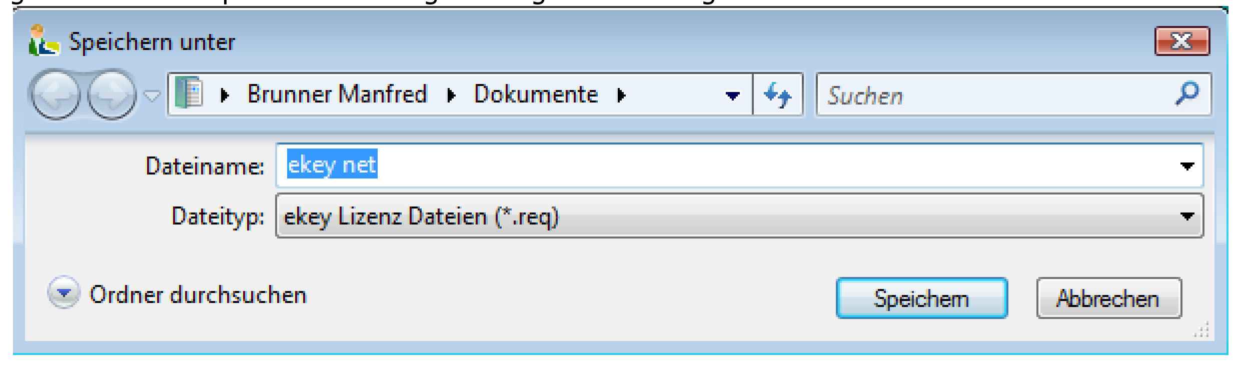
Online Aktivierung

Im Gegensatz zur Offline-Aktivierung läuft alles weitere automatisch ab. Am Ende der Aktualisierungssequenz, wird im Informationsfeld festgehalten, dass die Lizenz aktiviert wurde.

ekey net business
Die Lizenz für ekey net business ist bereits aktiviert worden
ekey net business ist uneingeschränkt verwendbar
ID: MIZHV-0VP11-4OPQG-RFZX9-0IUK3
Lizenz Anzahl: 30
Erstellt: 02.03.2010, 10:20:57

Offline Aktivierung

Bei der Offline-Aktivierung wird eine Lizenz-Datei erzeugt. Diese können Sie an einem beliebig gewünschtem Speicherort ablegen. Folgender Dialog erscheint dazu am Bildschirm

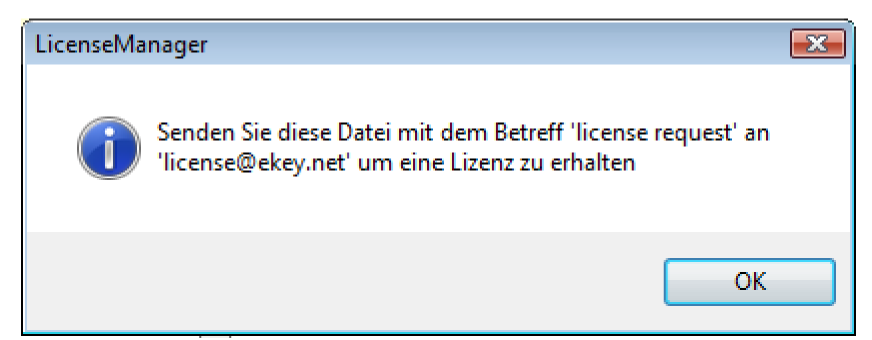


Nach Klick auf Speichern erfolgt die Information, dass ein Email mit

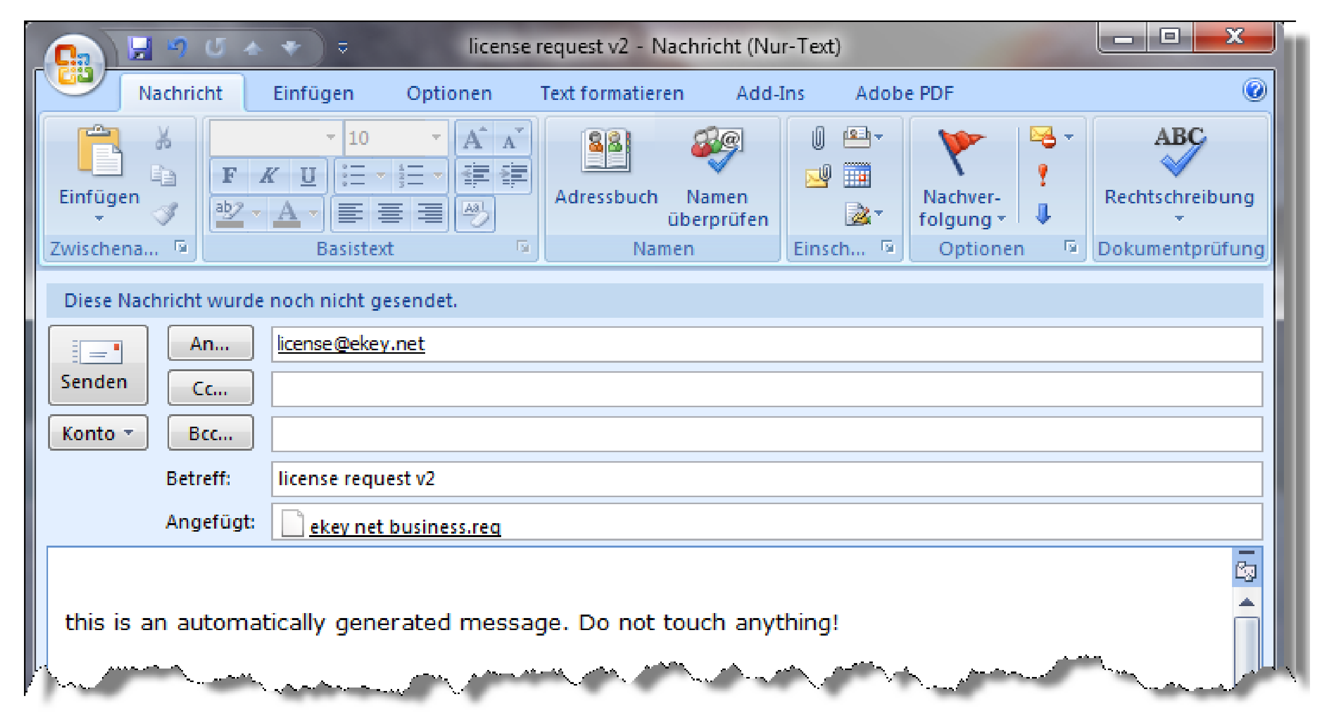
- der Betreffzeile „license request"
- an die Adresse license@ekey.net
- mit dem Attachement *.req (zuvor gespeichertes Request-File)

zu senden ist.





Verwenden Sie für Ihren Emailverkehr MS Outlook, so öffnet es sich automatisch und alle notwendigen Daten werden eingetragen. Sie brauchen das E-Mail nur mehr abzusenden.



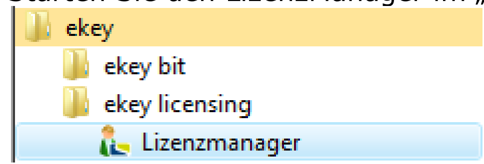
Verändern Sie das Email oben nicht und senden Sie es durch Klick auf den Buttonab.

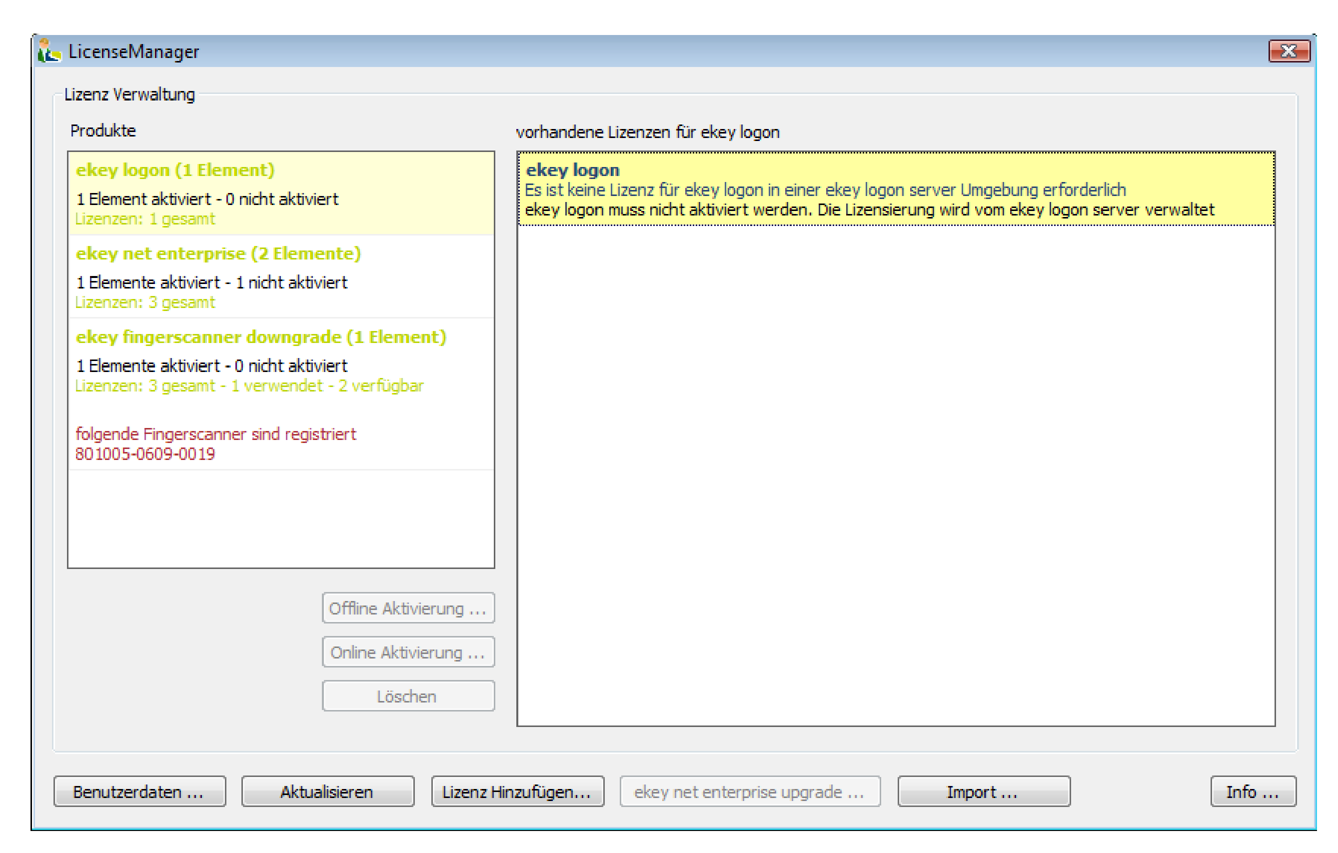
Verwenden Sie einen anderen Mailclient als MS Outlook zum Mailversand, so starten Sie diesen und senden Sie ein Email mit folgendem Inhalt ab:
AN: license@ekey.net
BETREFF: license request V2
Fügen Sie die zuvor erstellte ekey Lizenz Datei (.req) an. Senden Sie anschließend das Mail ab.

ekey erhält nun das Mail und sendet Ihnen den aktivierten Lizenz-Container retour. Sie erhalten also nach einiger Zeit, max. 1-2 Tage, die aktivierten Lizenzen in Form einer Datei (*.act) retour.

Diese von ekey retournierte Datei (*.act) speichern Sie wieder an einem beliebigen Ort ab.

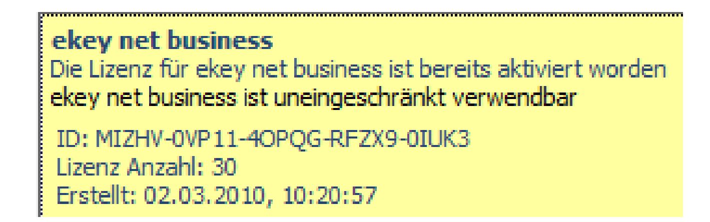
Starten Sie den LizenzManager im „**Startmenü**" -> „**Programme**"-> „ekey" mit einem Klick.





Klicken Sie dann auf [Import ...] und wählen Sie die aktivierte Lizenzdatei (*.act) die Sie von ekey retour erhalten und abgelegt haben aus.

Die Aktivierung des Lizenzpaketes sehen Sie dann im LizenzManager



Damit ist die Offline-Aktivierung abgeschlossen.



Informationen zu den Lizenzen

Öffnen Sie den ekey LizenzManager aus dem Startmenü. Sie können folgende Informationen zu den einzelnen ekey Lizenzpaketen ablesen:

LicenseManager

Lizenz Verwaltung

Produkte

ekey logon (1 Element)
1 Element aktiviert - 0 nicht aktiviert
Lizenzen: 1 gesamt

ekey net enterprise (2 Elemente)
1 Elemente aktiviert - 1 nicht aktiviert
Lizenzen: 3 gesamt

ekey fingerscanner downgrade (1 Element)
1 Elemente aktiviert - 0 nicht aktiviert
Lizenzen: 3 gesamt - 1 verwendet - 2 verfügbar

folgende Fingerscanner sind registriert
801005-0609-0019

vorhandene Lizenzen für ekey fingerscanner downgrade

ekey fingerscanner downgrade
Die Lizenz für ekey fingerscanner downgrade ist bereits aktiviert worden
ekey fingerscanner downgrade ist uneingeschränkt verwendbar
ID: ZJ5IN-4N2PQ-1K5UA-VBIW4-NYM4C
Lizenz Anzahl: 3
Erstellt: 17.09.2009, 14:48:45

- Hier sehen Sie den Status des Lizenzpaketes aktiviert/nicht aktiviert)
- Datum/Uhrzeit der Erstellung des Lizenzpaketes
- Die Paketgröße
- Lizenznummer

Offline Aktivierung ... | Online Aktivierung ... | Löschen

Benutzerdaten ... | Aktualisieren | Lizenz Hinzufügen... | ekey net enterprise upgrade ... | Import ... | Info ...

Hier sehen Sie die

- **Art des Lizenzpaketes**: ekey fingerscanner downgrade
- **Größe des Lizenzpaketes**: z.b. hier ein 3er Paket
- **Anzahl der dafür bereits registrierten Fingerscanner**(= verbrauchte Lizenz)

- ekey net Lizenzen können maximal 3 mal aktiviert werden (online oder offline). Notwendig ist dies z.B. bei einer Neuinstallation aufgrund einer Übersiedlung usw. Ab einer 4. Aktivierung müssen Sie mit ekey Kontakt aufnehmen.

- Die Lizenzdaten werden in Verbindung mit den Betreiber-Daten (Benutzerdaten) bei ekey gespeichert. Wichtig ist dabei, dass Sie sich die Emailadresse, unter der die Lizenz aktiviert wurde, unbedingt merken. Sie können die Lizenzen unter einer neuen Emailadresse **NICHT**erneut aktivieren!!

- Archivieren Sie unbedingt die mitgelieferten Lizenz-Codes an einem geeigneten Ort (sicher gegen unbefugten Zugriff, usw). Sie brauchen diese unter Umständen bei Systemdefekten oder Zerstörung des Systems (Brand, usw) oder auch bei einem Transfer der Anlage auf neue Zielrechner erneut!

4 Geräte

ekey net verbindet eine Vielzahl von Geräten zu einem Gesamtsystem, welches zentral mit der Software ekey net verwaltet wird. In den folgenden Kapiteln lernen Sie die einzelnen Geräte und deren Aufgabe im Gesamtsystem kennen.

4.1 Gerätearten

Folgende Geräte können Sie in ekey net betreiben:



Die Liste der Gerätetypen spiegelt den Stand zum Zeitpunkt der Erstellung dieses Handbuches wider. Es kommen im Laufe der Zeit immer wieder neue Gerättypen dazu. Klären Sie mit ekey direkt, welche Gerätetypen zur Verfügung stehen.

Gerätebeschreibung	Symbol	Leistung	Beschreibung
ekey net S FSAP		40 Finger	Aufputzmontage für Außeneinsatz geeignet
ekey net M FSAP		200 Finger	Aufputzmontage für Außeneinsatz geeignet
ekey net L FSAP		2000 Finger (200 Finger in ekey net light)	Aufputzmontage für Außeneinsatz geeignet
ekey net S FSIN		40 Finger	Montage in Türblatt/Türstock oder Unterputz mit Einbauset für Außeneinsatz geeignet
ekey net M FSIN		200 Finger	Montage in Türblatt/Türstock oder Unterputz mit Einbauset für Außeneinsatz geeignet
ekey net L FSIN		2000 Finger (200 Finger in ekey net light)	Montage in Türblatt/Türstock oder Unterputz mit Einbauset für Außeneinsatz geeignet
ekey net S FSRFID		40 Finger + RFID Interface	RFID-Funktionen Aufputzmontage für Außeneinsatz geeignet
ekey net M FSRFID		200 Finger + RFID Interface	RFID-Funktionen Aufputzmontage für Außeneinsatz geeignet
ekey net L FSRFID		2000 Finger + RFID Interface (200 Finger in ekey net light)	RFID-Funktionen Aufputzmontage für Außeneinsatz geeignet
Feller net S (M,L)FS UP		40/200/2000 Finger	Unterputzmontage Für Außeneinsatz geeignet
Feller net S (M,L) FS UPREL		40/200/2000 Finger	Unterputzmontage Für Innenbereich
FSB net S (M,L) FS UP		40/200/2000 Finger	Montage auf Tür Für Außeneinsatz

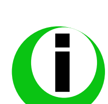
Gerätebeschreibung	Symbol	Leistung	Beschreibung
ekey net 3 SE AP		3 potentialfreie Relais	Aufputz- oder Hutschienenmontage nur für Innenbereich
ekey net 2 SE IN		2 H-Relais wahlw. potentialfrei	Montage in Türstock oder Türblatt nur für Innenbereich
ekey net 1SEmini		1 H-Relais	Aufputz – oder Hutschienenmontage nur für Innenbereich
ekey CVWIEG		RS485 <–> Wiegand	Aufputz – oder Hutschienenmontage nur für Innenbereich
ekey net SE REG		4 potentialfreie Relais	Hutschienenmontage
ekey net Terminalserver			
ekey CVLAN		RS485 <–> Ethernet	

ekey bit

ekey bit		USB-Fingerscanner	Fingeraufnahme im ekey net über USB



Unter Abschnitt 3.3 ist zusehen, dass die im ekey net konfigurierbaren Geräte (Terminals) vom gewählten Lizenzmodell abhängen. Achten Sie bitte darauf, dass Sie nicht ein Gerät erwerben, welches in ihrem ekey net Lizenzmodell nicht funktionsfähigist.



Um die Installation (Montage, elektrischer Anschluss) der Geräte ordnungsgemäß durchzuführen, beachten Sie bitte die Hinweise in den mit den Geräten mitgelieferten

- *Montage- und Installationsanleitung 801066*
- *Montage- und Installationsanleitung 801067*
- *ekey_net_Spezifikation.pdf*

4.2 Aufgaben der Geräte im ekey net

Die einzelnen Geräte haben im ekey net unterschiedliche Aufgaben. Um die Konfiguration im ekey net zu verstehen und einfacher und durchschaubarer zu machen, sollten Sie dieses Kapitel unbedingt durcharbeiten.

4.2.1 ekey net FS (Fingerscanner)



ekey net FS sind biometrische Sensoreinheiten, die die Fingerprints der Benutzer erfassen, auswerten und darauf folgend **Ereignisse** auslösen.
Die ekey net FS

- erfassen die Fingerprints (Ziehen des Fingers über den Sensor)
- errechnen Templates aus dem erfassten Fingerbild
- vergleichen den erfassten Fingerprint mit den berechtigten Fingertemplates, welche im Fingerscanner abgelegt sind
- speichern die berechtigten Finger-Templates
- speichern die Benutzer ID
- speichern die Zutrittsbeschränkungen (Zeitbereiche, Kalender usw.)
- speichern die Ereignisdefinitionen
- **lösendefinierte Ereignisse in Abhängigkeit dererfassten Finger und Zutrittsbeschränkungen aus.**

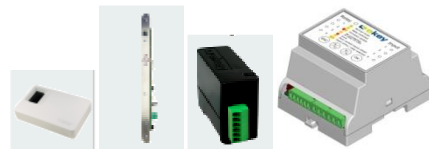
Zieht man einen Finger über den Sensor, so führt dies zu einem Ereignis. Welches Ereignis das ist, muss im ekey net aber vorher definiert werden. Ereignisse werden immer einem Finger zugeordnet. Ein Finger kann grundsätzlich nur ein Ereignis auslösen.

4.2.2 LED Signalisierung an den Fingerscannern:

Aufputz	Integra	Status-anzeige	Funktions -anzeige	.1 Beschreibung
		Orange blinkend	**Aus**	Es besteht keine Verbindung zu einen ekey CV LAN und einem ekey net Terminalserver - "Offline - Zustand". Bitte Prüfen Sie die Verbindungen.
		Aus	**Links: aus Rechts: Grün**	Der ekey CV LAN ist online, aber der ekey net Terminalserver ist nicht erreichbar. Prüfen Sie die Netzwerkver-bindungen und den ekey net Terminalserver Dienst.
		Aus	**Links: Grün Rechts: Grün**	Das System ist online - alle Komponenten kommunizieren korrekt.
		Orange blinkend	**Links: Grün Rechts: Grün**	Fingererkennung: Prüfung läuft
		Grün	**Links: Grün Rechts: Grün**	Fingererkennung: Positiv
		Rot	**Links: Grün Rechts: Grün**	Fingererkennung: negativ oder erkannter Finger abgelehnt

		Rot blinkend	**Links: Grün Rechts: Grün**	Datenabgleich mit dem Server
		Aus	**Abwechse lnd Links Rechts Grün blinkend**	Firmware Update wird durchgeführt
		Rot Grün blinkend	**Links: Grün Rechts: Grün**	2 Finger oder 2 Personenmodus: Das Gerät wartet auf den 2. Finger
		Rot Orange blinkend	**Links: Grün Rechts: Grün**	Wartezeit auf die ausgelöste Reboot-Aktion des Fingerscanners
Während des Bootvorganges:				
		Gelb	**Aus**	Moduldatenbank wird initialisiert
		Grün - Gelb	**Aus**	Flashfehler - eine automatische Reparatur wird gestartet
		Rot - Rot - Gelb	**Aus**	Flashfehler - der Fingerscanner muss getauscht werden - bitte mit dem Support Kontakt aufnehmen.
		Rot Grün blinkend	**Aus**	Die Kommunikation mit dem Sensor war während des Bootvorganges nicht möglich - bitte mit dem Support Kontakt aufnehmen.

4.2.3 ekey net SE (SE) – ekey net verbund SE



Die ekey net SE und der ekey net CV WIEG sind **Aktor**einheiten. Diese Einheiten führen eine **Aktion** aus: z.B. Schaltimpuls von 3secRelais 1 = Impuls Anschluss 1.ekey net SE

- schalten Ausgangsrelais- oder Halbleiterausgänge
- schalten Impuls – oder dauernd
- senden Daten an Fremdsysteme (z.B. Wiegand)
- geben Rückmeldungen ins System über digitale Eingänge (ekey net SE Mini)

Die **Aktionen,** die die SE auslösen, sind in der Softwareanwendung ekey net zu definieren und sind für deren Ausführung auf der ekey net SEimmer einem Ereignis zugeordnet.

Mithilfe einer **ekey net verbund SE** kann die Anzahl der schaltbaren Relais von bis zu max. 4 Relais auf 1 ekey net SE (Variiert je nach Modell von 1 bis 4) auf bis zu **max. 28** Relais mit 7 ekey net SE im Verbund erhöht werden. Siehe Kapitel6.6.3.2.2.

4.2.4 7-Segment Anzeigen der Steuereinheiten

Anzeige	Info	Beschreibung
	Beide Punkte leuchten	Das Terminal ist neu und wurde noch nicht initialisiert. Zustand kann durch Druck auf die Tasten Links und Rechts erzwungen werden.
	"r" im rechten Segment und Punkte blinken abwechselnd	Dieses Terminal wurde in einem anderen ekeynet System initialisiert. Rücksetzung durch Druck auf die Tasten Links und Rechts erforderlich.
	"o" im rechten Segment	Es besteht keine Verbindung zu einem ekey CV LAN und einem ekey net Terminalserver - "Offline - Zustand". Bitte Prüfen Sie die Verbindungen.
	Punkt blinkt links	Der ekey CV LAN ist online, aber der ekey net Terminalserver ist nicht erreichbar. Prüfen Sie die Netzwerkverbindungen und den ekey net Terminalserver Dienst.
	Punkte blinken abwechselnd	Das System ist online - alle Komponenten kommunizieren korrekt.

© 2010 – ekey biometric systems GmbH



4.2.5 ekey bit

Das ekey bit ist ein USB-Fingerscanner, der im ekey net zur erstmaligen oder wiederholten Fingeraufnahme (Erfassung der Fingertemplates jedes Benutzers) verwendet wird.

4.2.6 ekey net CV (converter) LAN



Der ekey net CV LAN ist minimalisiert betrachtet ein Daten-Konverter der

- die physikalische Umsetzung von RS485 auf Ethernet vollzieht
- der die Verwaltung der ihm zugeordneten Geräte auf RS485 – Seite übernimmt

Ein ekey net CV LAN kann maximal 8 Geräte am RS485 Bus verwalten, wobei es dabei unerheblich ist, welcher ekey net Gerätetyp (Fingerscanner, Steuereinheit,..)angeschalten wird.

4.2.7 ekey net Terminalserver



Der ekey net Terminalserver ist ein Systemdienst der auf einem PC / Server mit einem Windows Betriebssystem arbeitet. Die Aufgaben dieses Dienstes sind:

- die Verwaltung der ihm zugeordneten Terminalgruppen und Geräte
- Servermatching
- Zwischenspeicherung von Logdaten
- Kommunikation mit dem ekey net Masterserver
- WEB - Logging

Welche Windows-Betriebssysteme für den Betrieb von ekey net Terminalserver geeignet sind, entnehmen Sie bitte der ekey net Spezifikation.

4.2.8 ekey net Masterserver



Der ekey net Masterserver ist ein MS Windows-Dienst, der auf einem PC / Server mit Windows Betriebssystem arbeitet. Im System darf nur 1 ekey net Masterserver vorhanden sein.Die Aufgaben dieses Dienstes sind:

- die Verwaltung der ihm zugeordneten Terminalserver
- Datenablage und Datenbankverwaltung

Welche Windows-Betriebssysteme für den Betrieb von ekey net Masterserver geeignet sind, entnehmen Sie bitte der ekey net Spezifikation.



4.2.9 ekey net Restore

Ab Version ekey net 4.1 gibt es das Programm „ekey net Restore“, Sie finden dieses unter Start/Programme/ekey/ekey net/

Dieses Tool ermöglicht Ihnen eine ältere Version Ihrer Konfiguration wiederherzustellen, falls versehentlich ein User gelöscht wurde oder die aktuelle Datei gelöscht wurde.

Sie müssen nur den Sicherungsordner auswählen und den Ordner wo Ihre aktuelle „ekey netdata“ sich normalerweise befindet.

Direkt im Programm können Sie die Dienste stoppen und die Datei wiederherstellen.

ekey net Restore

Um eine Sicherung der ekey net Datei wiederherzustellen, wählen Sie das Sicherungsverzeichnis mit den gesicherten ekey net Dateien und das Zielverzeichnis aus.
Anschließend wählen Sie eine Datei aus der Liste aus und drücken die Schaltfläche "Sicherung wiederherstellen" zur Wiederherstellung der Sicherung.
Hinweis: Der Dienst des Master Servers muss gestoppt sein!

Sicherungsverzeichnis: C:\ekey net DB\Backup [Auswählen ...]

Zielverzeichnis: C:\ekey net DB [Auswählen ...]

Sicherungen:

Name v	Datum
20110512162139ekey net.netdata	05/12/11 16:21:39
20110512162011ekey net.netdata	05/12/11 16:20:11
20110512143659ekey net.netdata	05/12/11 14:36:59
20110512143637ekey net.netdata	05/12/11 14:36:37
20110512094923ekey net.netdata	05/12/11 09:49:23
20110512092502ekey net.netdata	05/12/11 09:25:02
20110512091537ekey net.netdata	05/12/11 09:15:37
20110512091344ekey net.netdata	05/12/11 09:13:44
20110512090925ekey net.netdata	05/12/11 09:09:25
20110512090653ekey net.netdata	05/12/11 09:06:53
20110511082837ekey net.netdata	05/11/11 08:28:37
20110511082829ekey net.netdata	05/11/11 08:28:29
20110511082647ekey net.netdata	05/11/11 08:26:47
20110511082553ekey net.netdata	05/11/11 08:25:53
20110511082505ekey net.netdata	05/11/11 08:25:05
20110511082454ekey net.netdata	05/11/11 08:24:54
20110511082412ekey net.netdata	05/11/11 08:24:12

Dateiinformationen:

Dateiname: 20110512162139ekey net.netdata

Lizenztyp: ekey net business

Anzahl der Benutzer: 4
Anzahl der Fingerscanner: 4

Informationen über Datei 'ekey net.netdata':

Dateiname: ekey net.netdata

Lizenztyp: ekey net business

Anzahl der Benutzer: 4
Anzahl der Fingerscanner: 4

Dienst Status

ekey net masterserver Status: Der Dienst ist gestartet. [Starten] [Stoppen]

ekey service guard Status: Der Dienst ist gestartet.

[Sicherung wiederherstellen] [Schließen]



5 Software Installation

5.1 Vorbereitung der Installation

Bevor Sie mit der Installation (sowohl Hardware als auch Software) von ekey net beginnen, empfehlen wir ihnen sich eine Systemübersicht und einen Plan zu machen. Dies wird ihnen bei der Inbetriebnahme und der Konfiguration ihres Systems helfen:

Definieren Sie bzw. ihre IT-Abteilung

- den physikalischenInstallationsort des ekey net Masterservers
- den physikalischenInstallationsort des (der) ekey net Terminalserver
- wie werden die ekey net CV LAN dem Terminalserver zugeordnet?
- welche Terminals (Fingerscanner, Steuereinheiten) sind welchem ekey net CV LAN zugeordnet?
- geben Sie jedem Gerät eine selbsterklärende, verständlicheBezeichnung!

Folgende Daten brauchen Sie zur Installation und Konfiguration (halten Sie dafür Rücksprache mit Ihrer IT-Abteilung bzw. Ihrem IT-Spezialisten). Erheben Sie vor Installationsbeginn diese Daten.

- Host (Computer) Name des ekey net Masterservers (ist von Ihnen bzw. Ihrer IT-Abteilung zu definieren)
- Host (Computer) Name des (der) ekey net Terminalserver (ist von Ihnen bzw. Ihrer IT-Abteilung zu definieren)
- IP-Adressen der ekey net CV LAN (ist von Ihnen bzw. Ihrer IT-Abteilung zu definieren)
- MAC-Adressen der ekey net CV LAN (finden Sie auf der Seriennummernetikette (12-stellig hexadezimal,z.B. 00 20 4a ba 12 0d)
- Seriennummern und Gerätetyp der Terminals (Fingerscanner, SE) finden Sie auf der Seriennummernetikette der Geräte (14-stellig, z.B. 80034020090004)

Die Mindestanforderungen an das Zielsystem, auf dem ekey net betrieben werden soll, finden Sie in der ekeynetSpezifikation.



Bevor Sie mit der Installation von ekey net auf ihrem Zielsystem starten, überprüfen Sie bitte folgende Einstellungen
Rechnerleistung(ekey_net__Spezifikation->Kapitel 4.1)
Betriebssystem (ekey_net_Spezifikation->Kapitel 2.2)
Netzwerkeinstellungen (ekey_net_Spezifikation ->Kapitel 2.3)
Verdrahtung / Montage (ekey_net_Spezifikation->Kapitel 4)

Im Netzwerk muss sichergestellt sein,

- dass dieRechner (Server), auf dem die Dienste ekey netMasterserver und ekey net Terminalserver sowie die Anwendung ekey net Admin mit Namen (DNS) wechselseitig erreichbar sind.
- dass die genannten Server zeitlich synchronisiert sind. Die Zeitabweichung unter den Rechnern (Server) darf nicht mehr als 10 Sekunden betragen (Sicherheitsfunktion)

Für die Durchführung der Installationskapitel wird davon ausgegangen, dass alle Geräte ordentlich verkabelt sind, an Spannung liegen und mit dem Netzwerk (Ethernet) verbunden sind.



5.2 Durchführung der Installation

5.2.1 Allgemeiner Ablauf der Installation

Installation des **ekey net Masterservers** siehe Kapitel 5.2.2

Installation des (der) **ekey net Terminalservers** siehe Kapitel 5.2.2

Installation des (der) **ekey net Admin** siehe Kapitel 5.2.2

Netzwerk-konfiguration der **ekey net CV LAN** siehe Kapitel 5.2.3

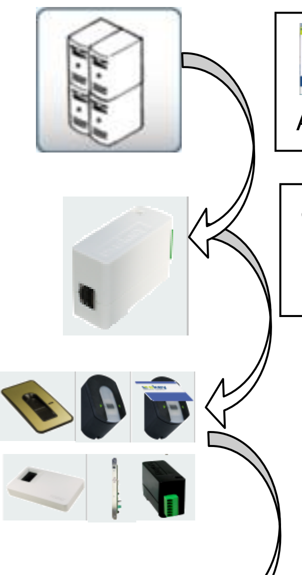
MODULUpdate der Geräte **ekey net** siehe Kapitel 5.2.4

Konfiguration und Administration des Systems **ekey net** Siehe Kapitel 6

Installation von

- ekey net Masterserver
- ekey net Terminalserver und
- ekey net Admin

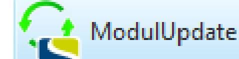
sowie der weiteren Komponenten (ekey converter LAN config…) von ekey net kann auch in einem Schritt erfolgen. Die Unterscheidung ergibt sich aus der physikalischen Position der Komponenten. Das heißt auf welchem physikalischen Server (Rechner / PC) die Komponenten zu betreiben sind.

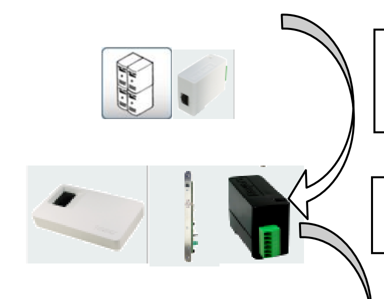


Software ekey net (Masterserver, Terminalserver ,ekey net Admin,…) installieren. Siehe dazu Kapitel 5

ekey converter LAN für Netzwerk-Betrieb konfigurieren. Verwenden Sie dazu das Tool ekey CONVERTER LAN config

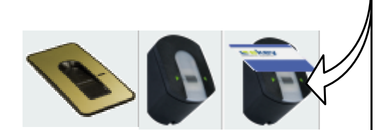
Firmwareversionsstände der Geräte prüfen und gegebenenfalls auf Stand bringen. Verwenden Sie dazu das Tool





ekey net Terminalserver und ekey net CV LAN mit Hilfe des ekey net Admin konfigurieren.

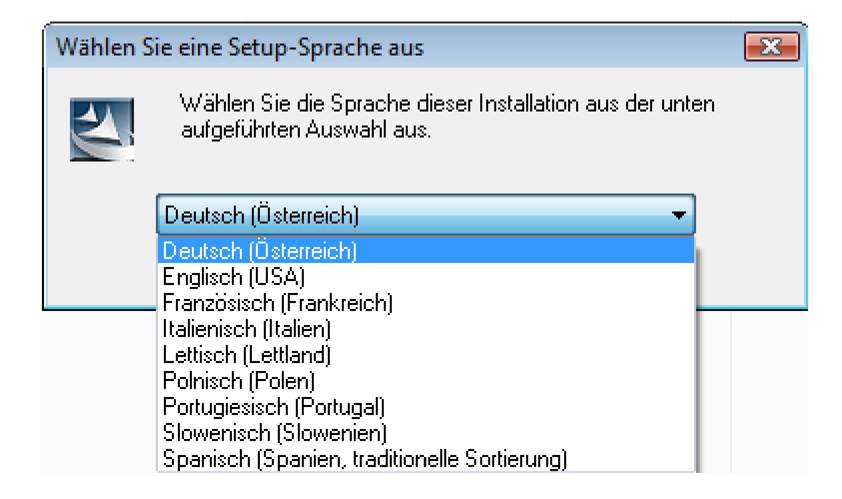
ekey net SE im ekey net Admin konfigurieren



ekey net FS im ekey net Admin konfigurieren und die ekey net SE dem Fingerscanner zuweisen. Auf dieser zugewiesenen Steuereinheit werden dann die in den Ereignissen definierten Aktionen ausgeführt.

5.2.2 Neu-Installation der ekey net Softwarekomponenten

Setup.exe starten
Nach dem Start von Setup.exe ist die Sprache auszuwählen. Folgendes Fenster erscheint hier, um die Auswahl zu treffen. Wählen Sie aus der Combobox die entsprechende Sprache und bestätigen Sie mit Klick auf den OK-Button.
Setup.exe erlaubt die komplette oder benutzerdefinierte Installation von *ekey net*



Danach startet der ekey net InstallShield Wizard



Bestätigen Sie hier mit Weiter >

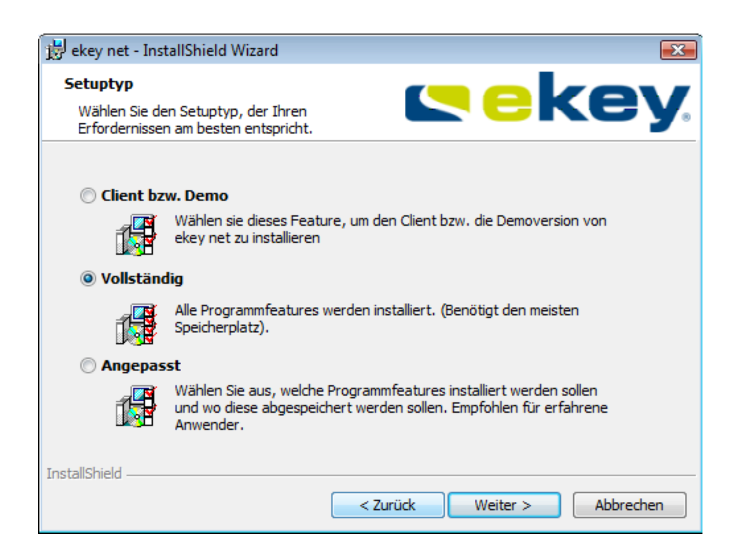
Es öffnet sich das Fenster mit dem Lizenzvertrag. Bitte lesen Sie diesen sorgfältig durch und bestätigen Sie durch Auswahl des Feldes

Ich akzeptiere die Bedingungen der Lizenzvereinbarung

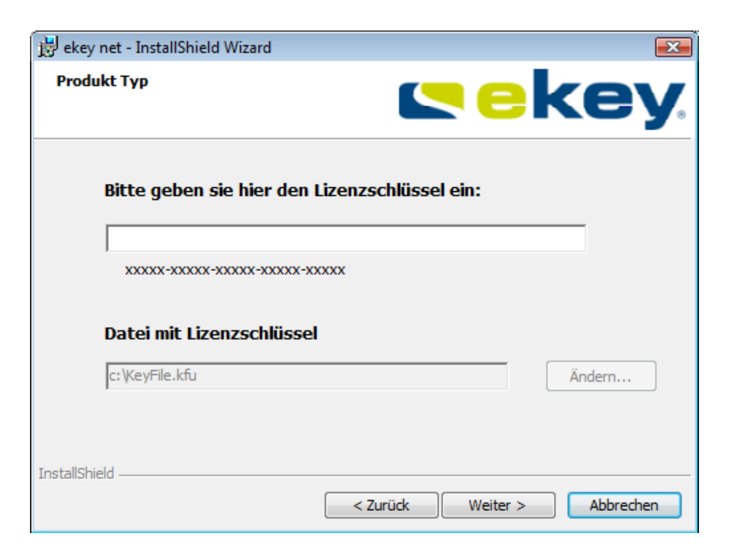
und anschließenden Klick auf Weiter >





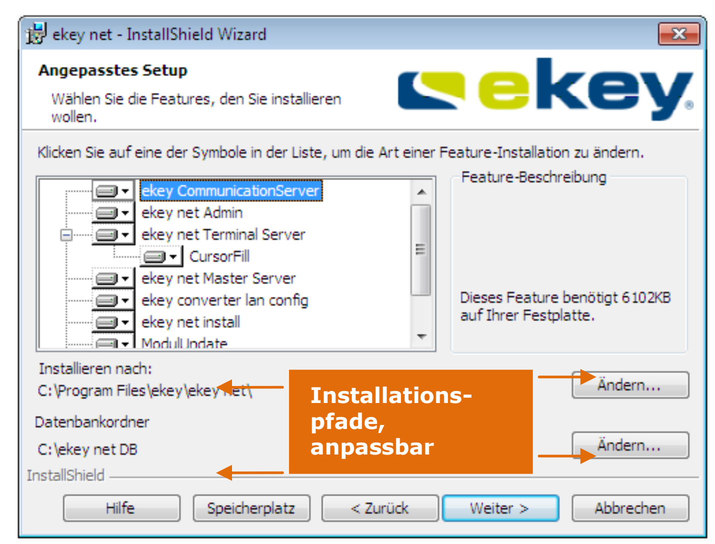


Geben Sie nun die Zeichenfolge eines Lizenzpaketes ein. Falls bereits Lizenzen aktiviert wurden. Erscheint das folgende Fenster nicht mehr !





Definition der Installationspfade



die Installationspfade können bei der Installation angepasst werden.

<u>StandardPfade für die Installation</u> (Werkseinstellung)
ekeynetAnwendungen: C:\Programme(Program Files)\ekey\ekey net
ekeynetDatenfile: C:\ekey netDB



Vermeiden Sie für den Datenbankordner die Verwendung von UNC – Pfaden oder Netzlaufwerken, um Probleme mit Berechtigungen zu vermeiden. Das Dienstkonto für den ekey net Masterserver Dienst muss Vollzugriff auf diesen Ordner haben!

Auswahl der zu installierenden Komponenten von ekey net
Folgende Komponenten müssen im Gesamtsystem für die einwandfreie Funktion von *ekey net*installiert werden.

- *ekey Communicationserver*
  Funktion:*ekey Communicationserver* verwaltet die ekeynet Kommunikation im Netzwerk auf Basis von MSMQ (Microsoft Message Queuing). Dieser Dienst muss auf jedem Rechner im ekeynet -System installiert werden. Dies gilt insbesondere für die Serverdienste *ekeynet Masterserver* und *ekeynet Terminalserver* als auch für den *ekey net Admin*.

- *ekeynet Admin*
  Funktion: Dieses Programm kann auf einer beliebigen Anzahl von Computern installiert sein und dient den ekeynet Administratoren zur Verwaltung und Parametrierung von ekeynet. Diese Softwareanwendung wird auch für den Portiermodus verwendet.

- *ekeynet Masterserver*
  Funktion: Datenbankverwaltung; hier werden alle Systemdaten (Personendaten, Terminaldaten, Zutrittsdaten, …) zentral abgelegt. Bei jeder ekeynet Installation darfnur **ein***ekeynet Masterserver* aktiv sein.

- *ekeynet Terminalserver*
  Kümmert sich um die Verteilung der Zutrittsdaten vom *ekeynet Masterserver* zu den Geräten und zurück, überwacht die Geräte, etc. Bei jeder Installation kann eine beliebige Anzahl von *ekeynet Terminalservern* aktiv sein (Beschränkungen durch das Betriebssystem sind möglich!).

- *ekeyconverterLAN config*
  listet die vorhandenen *ekey net CVLAN* im lokalen Netzwerk und erlaubt die Netzwerkkonfiguration und Firmwareupdates der einzelnen *ekey net CVLAN.*

- *ekey ModuleUpdate*
  ist eine Softwareanwendung zum Firmware-Update der Geräte (ekey net SE, ekey net CV WIEGund ekey net FS)
- *ekey ServiceGuard*
  Dieser Dienst wird automatisch installiert und überwacht die ekey net Serverdienste:
  - ekey net Communicationserver
  - ekey net Masterserver
  - ekey net Terminalserver

  Im Falle eines Problems werden die Dienste automatisch neu gestartet!



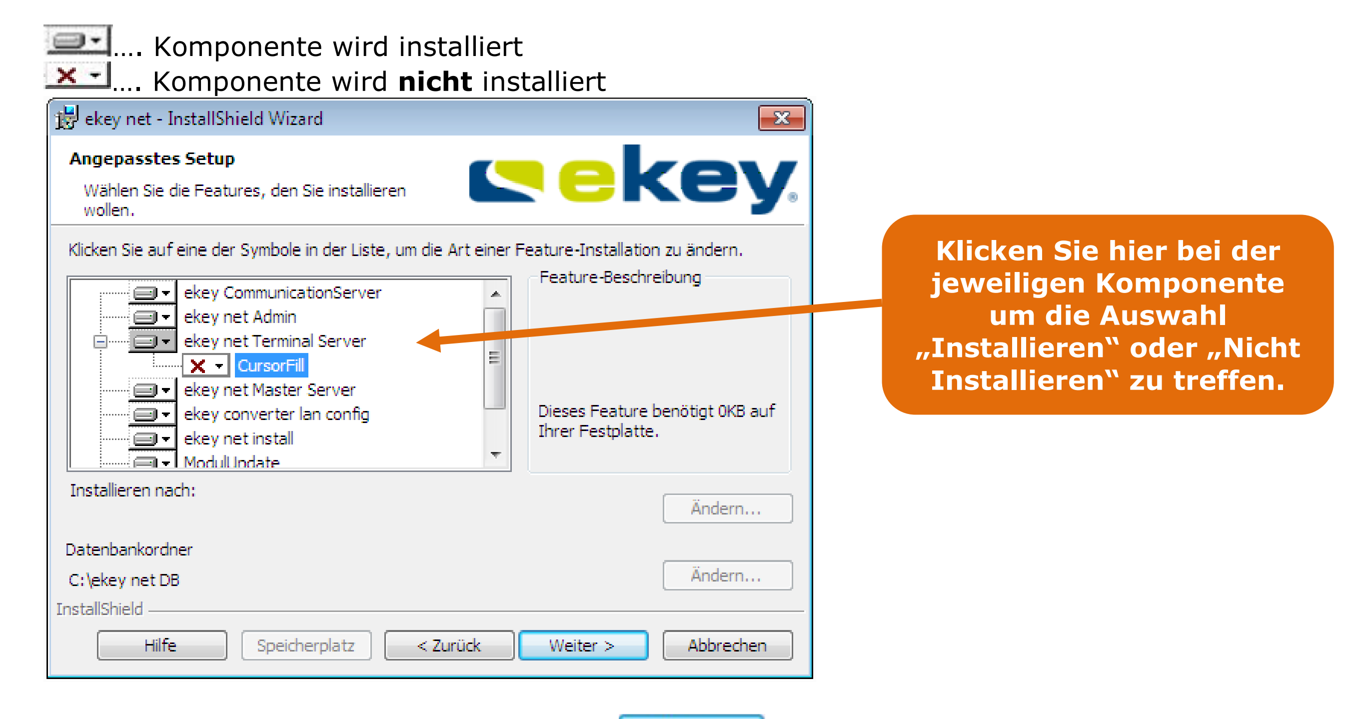
Sollen ekey net Systemdienste zu Wartungszwecken gestoppt werden, müssen Sie ***vorher den ekey Service Guard stoppen!***

Folgende Programmteile können, falls die Funktion benötigt wird, zusätzlich installiert werden:

- *ekey CursorFill*
  Die einfachste Schnittstelle zu Fremdsoftware wie beispielsweise Zeiterfassung o. ä.. CursorFill benötigt am selben Rechner den *ekeynet Terminalserver*. Bei Zutrittsaktivitäten wird die konfigurierte Benutzer-ID in das Feld des Cursors am Desktop gesetzt. Vergleichbar ist diese Funktion mit einem Barcodescanner, der nach dem Lesen des Barcodes die Nummer in das Feld des Cursors setzt. CursorFill muss nicht installiert werden, wenn die Funktion nicht benötigt wird.

Softwarekomponenten	Art	Größe	Abhängigkeiten von Diensten / Treibern / Ladegruppen
ekeynetadmin.exe	Anwendung	4,56 MB (4.792.230 B)	• ekey net Masterserver • ekey net Terminalserver • ekey Communicationserver
ekey net Admin Hilfe	PDF		• ekey_net_Handbuch
ekeyres_DEU.dll	Programmbibliothek	5,01 MB (5.257.728 B)	• Deutsche DLL für ekeynetAdmin.
ekeySvcGuard.exe	Dienst	341 KB (349.696 B)	• Überwacht die ekey net Server Dienste
ekeynetterminalserver.exe	Dienst	1,13 MB(1.185.792 B)	• ekey Service Guard • ekeyCommunicationserver
ekeynetmasterserver.exe	Dienst	1,38 MB(1.455.616 B)	• ekey Service Guard • ekey Communicationserver
ekeyCommunicationServer.exe	Dienst	1,20 MB(1.258.496 B)	• MSMQ
ekeynetcursorfill.exe	Anwendung	1,13 MB(1.186.816 B)	• ekeynet Terminalserver
ConfigConverter.exe	Anwendung	1,25 MB(1.316.352 B)	• ekeynet Terminalserver und ekey Service Guard müssengestoppt sein
ModuleUpdate.exe	Anwendung	1,55 MB(1.631.232 B)	• ekey Communicationserver • ekeynet Terminalserver und ekey Service Guard müssen gestoppt sein
KSniffer.exe	Anwendung	352 KB (360.448 B)	• Keine

Die Auswahl, ob eine Programmkomponente auf dem entsprechenden Zielrechner (Server) installiert wird oder nicht,machen Sie ebenfalls im **ekey net InstallShield Wizard**

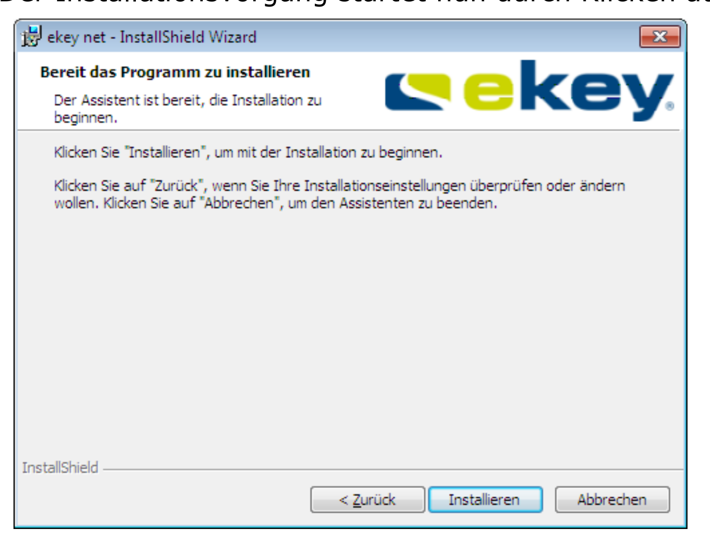


Bestätigen Sie dann die Einstellungen und Weiter >



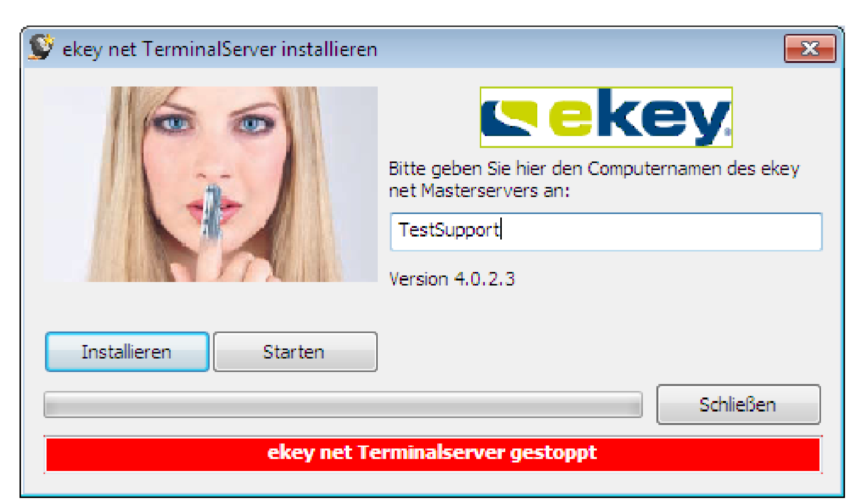
Installieren Sie bei jedem ekey net Terminalserver auch das Programm ekey CONVERTER LAN config *und* ModulUpdate *Sie brauchen diese Anwendungenspäter für die Gerätekonfiguration.*

Der Installationsvorgang startet nun durch Klicken auf Installieren





Der Vorgangkann einige Minuten dauern. Am Ende erscheint, sofern Sie am Rechner einen Terminalserver installiert haben, folgendesFenster:

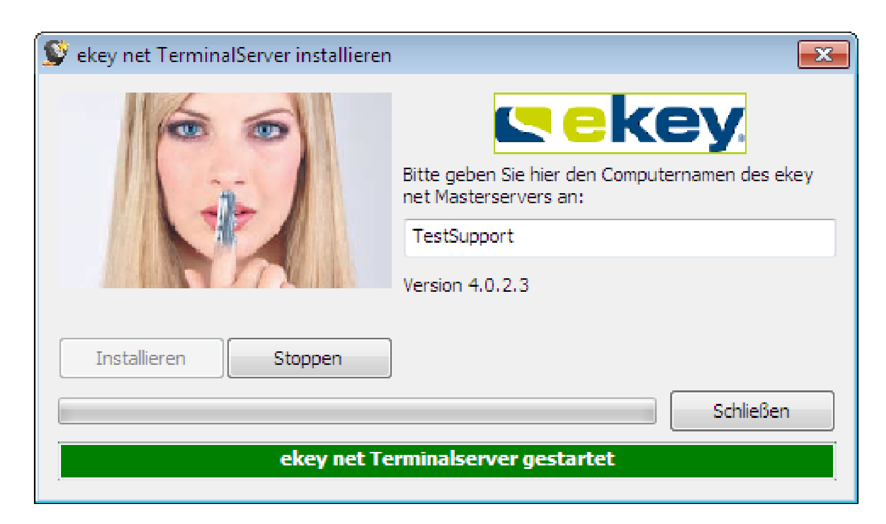


Damit der ekey net Terminalserver mit dem richtigen ekey net Masterserver kommunizieren kann, muss dieser entsprechend zugewiesen werden. Dies erfolgt im obigen Fenster. Der Name des Rechners (HOSTNAME), auf dem der ekey net Masterserver läuft, ist hier einzugeben.



Die Verwendung einer IP-Adresse oder „localhost" kann zu Fehlfunktionen führen

Durch anschließendes Klicken auf „**Installieren**" wird der ekey net Terminalserver fertig installiert und gestartet. Das Setupist damit für diesen Rechner abgeschlossen.



Wiederholen Sie nun die Installation auf den weiteren physikalischen Rechnern (Servern) mit den dort notwendigen Softwarekomponenten von ekey net.



*Achten Sie unbedingt darauf, dass Sie**nur einen ekey net Masterserver** installieren! Das System ekey net funktioniert ansonsten nicht entsprechend der Spezifikation*

Haben Sie alle Softwarekomponenten auf den Zielrechnern/ Serverninstalliert, dann beginnen Sie nun mit der Konfigurationder ekey net CV LAN.



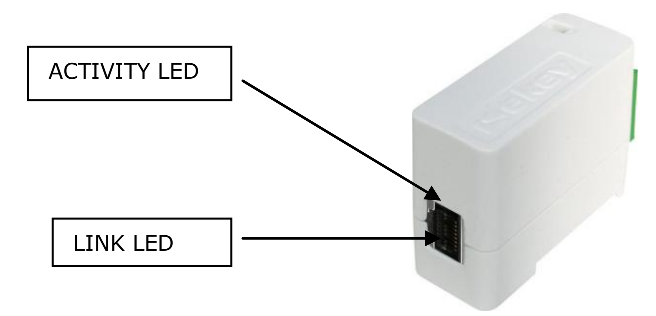
5.2.3 ekey net CV LAN

5.2.3.1 Optische Signalisierung

Damit Sie im Vorfeld prüfen können, ob der ekey net CV LAN

- Mit Spannung versorgt ist
- Mit dem Netzwerk (Ethernet) verbunden ist

sind 2 Leds am ekey net CV LAN ausgeführt die folgende Bedeutung haben:



ekey net CV LAN hat 2 Statusanzeigen (LEDs) zur Signalisierung der

LINK LED

Farbe	**Bedeutung**
Aus	Keine Verbindung
Amber (Orange)	10Mbps
Grün	100Mbps

ACTIVITY LED

Farbe	**Bedeutung**
Aus	Keine Aktivität
Amber(Orange)	Half Duplex
grün	Full Duplex

5.2.3.2 Konfiguration

Bevor Sie mit der Benutzer- und Terminal-Konfiguration im ekey net Admin starten können, müssen Sie noch die ekey net CV LAN einzeln der Reihe nach für ihr Netzwerk konfigurieren. Verwenden Sie dazu die Anwendung:





Bevor Sie starten stellen Sie noch sicher, dass alle im System laufenden Dienste ***ekey Service Guard und ekey net Terminalserver*** *beendet (gestoppt) sind! Die Anwendung ekey converterLAN config arbeitet ansonsten nicht zuverlässig!*

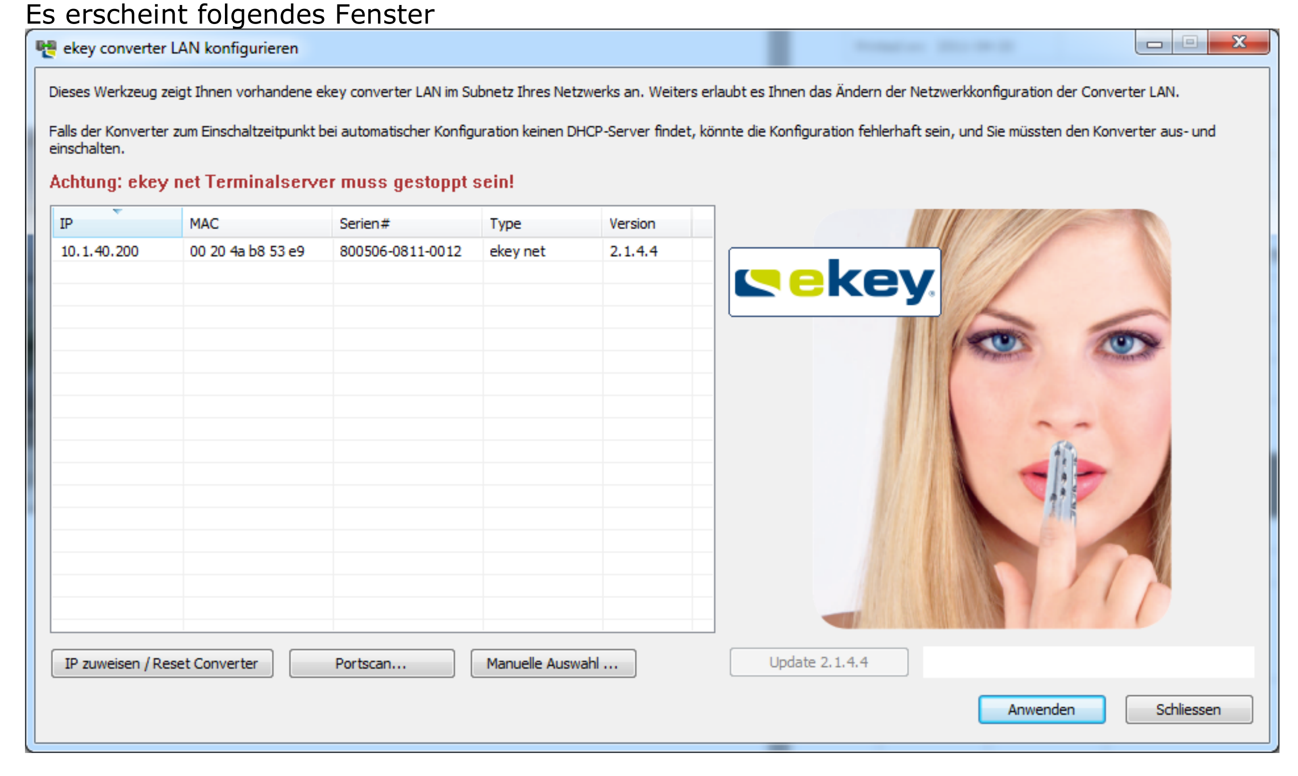


ekey net CV LAN werden ab Werk mit einer definierten IP-Adresse (**192.168.1.250)** ausgeliefert. Sollten Sie mehrere Converter einsetzen beachten Sie bitte, dass diese der Reihe nach angeschlossen und sofort auf eine andere IP-Adresse umprogrammiert werden müssen, sonst würde es zu Netzwerk- bzw. IP - Konflikten kommen.

Starten Sie nun das Programm



zur Konfiguration der ekey net CV LAN
Es erscheint folgendes Fenster



Nach einigen Sekunden erscheinen der Reihe nach die im Netzwerk (Ethernet) angebundenen ekey net CV LAN mit den Informationen:

- IP-Adresse
- MAC-Adresse



- Seriennummer
- Type
- Versionsnummer der Firmware

ekey net CV LAN die sich außerhalb des definierten Subnetzes befinden, sind (sofern Sie nicht geroutet sind) hier rot dargestellt. ekey net CV LAN in fremden gerouteten Netzen sehen Sie hier nicht!



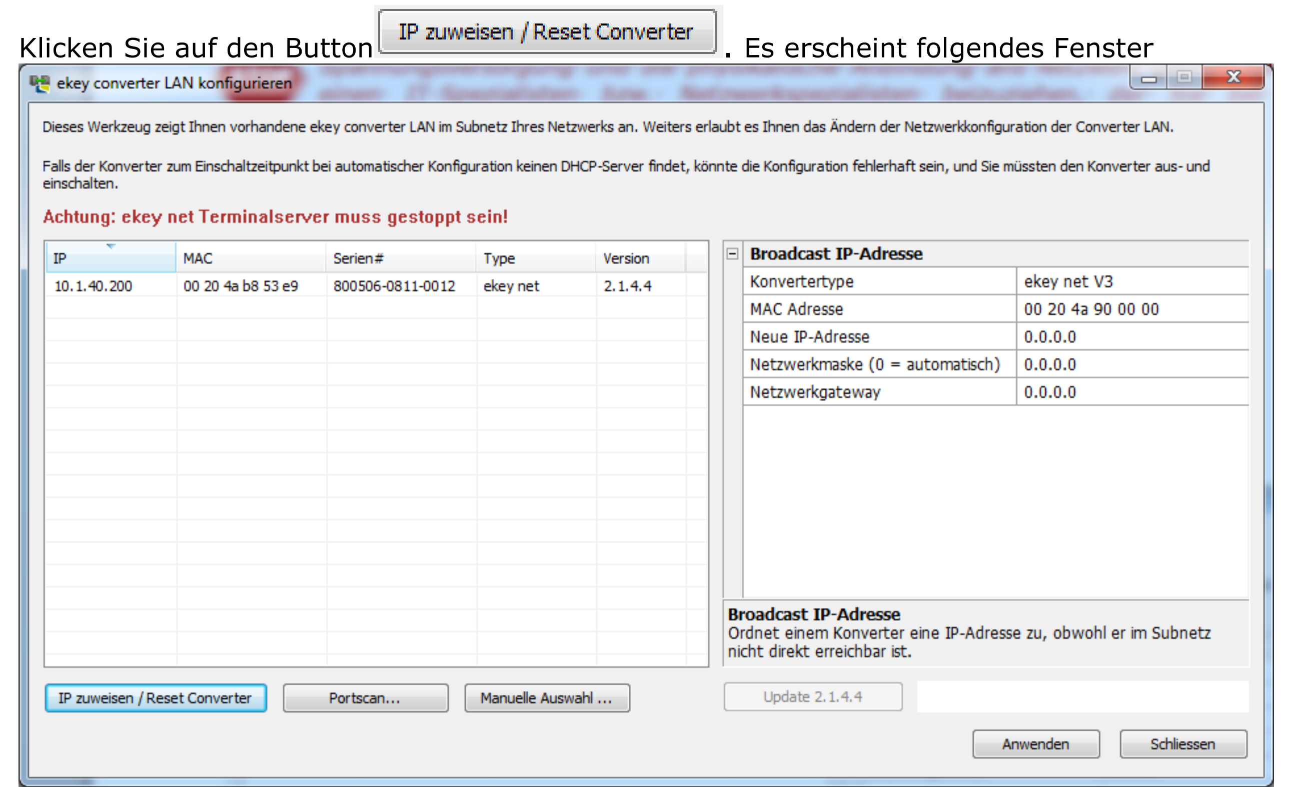
Sehen Sie hier nicht alle ekey net CV LAN gelistet, empfehlen wir, nachdem Sie die Spannungsversorgung und die physikalische Anbindung ans Netzwerk geprüft haben, einen IT-Spezialisten bzw. Netzwerkspezialisten beizuziehen, der Sie bei der Einrichtung des Netzwerks unterstützt.

5.2.3.2.1 Zuweisung einer neuen IP-Adresse

Die Zuweisung der IP-Adresse kann auf 2 Arten erfolgen:

5.2.3.2.1.1 IP-Zuweisen über MAC–Adresse

Klicken Sie auf den Button IP zuweisen / Reset Converter. Es erscheint folgendes Fenster



Bei dieser Art der Zuweisung erfolgt ein sogenannter „Broadcast" und man nutzt diese techn. Möglichkeit der Netzwerkkommunikation, um die IP-Adresse an ekey net CV LAN, die nicht im gleichen Subnetz sind, zu setzen. Für diese Variante müssen Sie die MAC-Adresse des ekey net CV LAN wissen, welche auf derSeriennummernetikette des ekey net CV LANzu finden ist.

Ablauf:

->Geben Sie die MAC-Adresse ein



->geben Sie die IP-Adresse, die Netzwerkmaske und eventuell ein Netzwerkgateway ein

->klicken Sie auf Anwenden

Nach einigen Sekunden erscheint der ekey net CV LAN mit der richtigen IP-Adresse in der Liste.



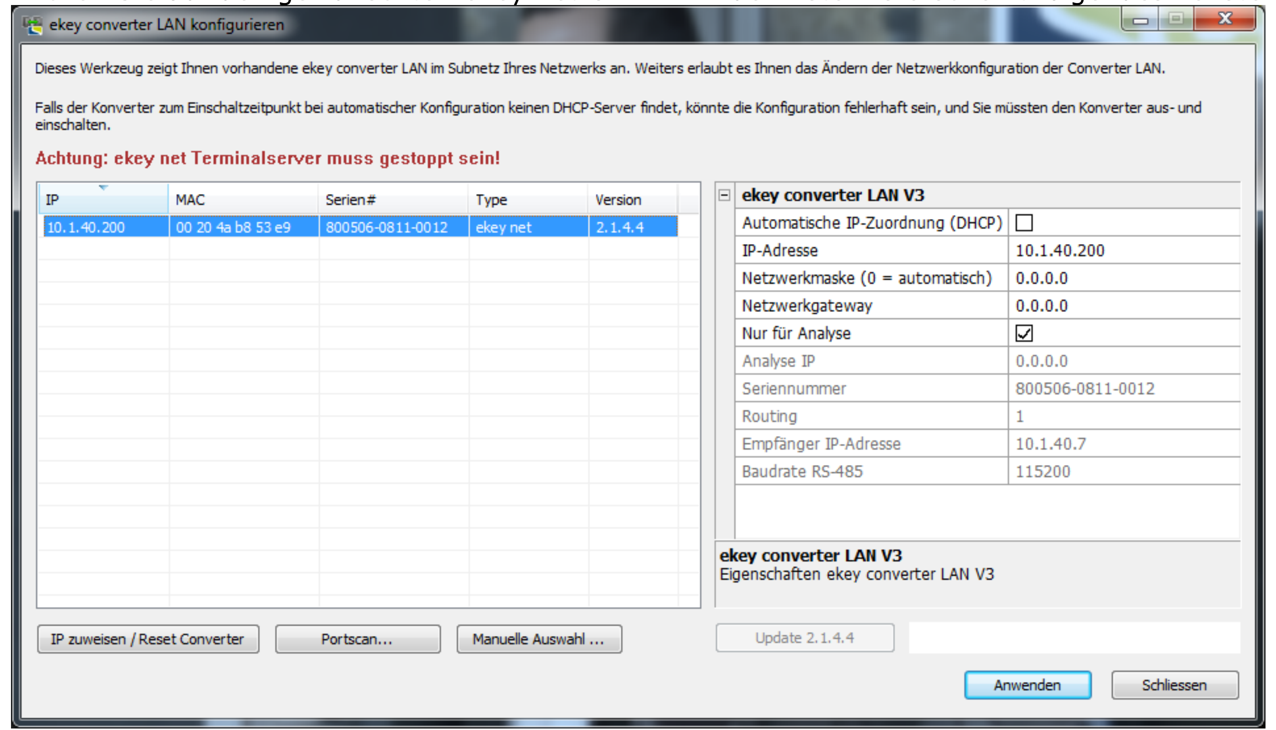
Erscheint der ekey net CV LAN nicht in der Liste, wiederholen Sie die Prozedur noch einmal. Sollte es immer noch nicht klappen, machen Sie den ekey net CV LAN kurz spannungslos und versuchen Sie es neuerlich.



Mit der Funktion „IP-zuweisen“ wird nach Ausführung am ekey net CV LAN ein Reset gemacht.

5.2.3.2.1.2 IP-Zuweisen durch Auswahl aus Liste

Klicken Sie auf den gewünschten ekey net CV LAN in der Liste. Es erscheint folgendes Fenster:



Ablauf:

-->geben Sie die IP-Adresse, die Netzwerkmaske und eventuell ein Netzwerkgateway ein



Die Checkboxen „Automatische IP-Zuordnung“ und „Nur für Analyse“ dürfen nicht gewählt sein!Sollte das Häkchen gesetzt sein, so entfernen Sie es durch einen Mausklick!

→klicken Sie auf 

Der ekey net CV LANverschwindet aus der Liste und taucht nach einigen Sekunden mit der neuen Netzwerkkonfiguration wieder auf.

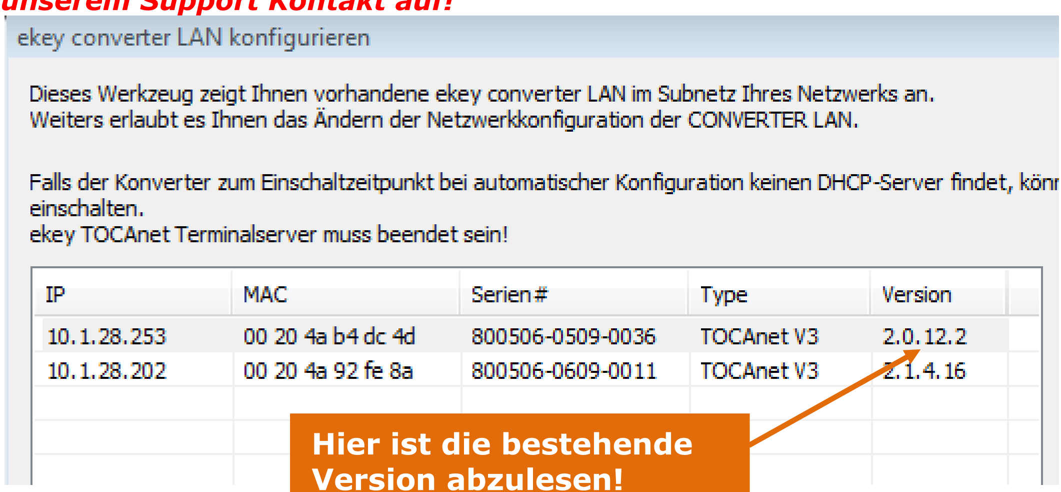
5.2.3.3 Firmwareupdateekey net CV LAN

Bei Auslieferung der ekey net Software wird auch die letztgültige Firmware-Version für die ekey net CV LAN mitgeliefert. Es kann vorkommen, dass die ekey net CV LAN selbst noch nicht mit dieser Version programmiert sind. Führen Sie bei Versionsmissstand einFirmwareupdate aus.

Wählen Sie dazu den ekey net CV LAN aus und klicken Sie auf Update 2.0.12.2.
Der Button ist nur aktiv, wenn der ekey net CV LAN netzwerktechnisch richtig konfiguriert – erreichbar ist und die Firmwareversion am ekey net CV LAN älter ist, als die im Button selbst angeführte Versionsnummer.



Beginnt die bestehende ekey converter Version lt. Anzeigemit 1. (z.B 1.6.1.16,) so führen Sie keinesfalls ein Update durch. Nehmen Sie vorher mit unserem Support Kontakt auf!





Trennen Sie den ekey net CV LAN während des Updates keinesfalls von der Spannungsversorgung. Dies kann zur Misskonfiguration des Gerätes führen und unter Umständen ist die Neukonfiguration nur im Werk (bei ekey) möglich.

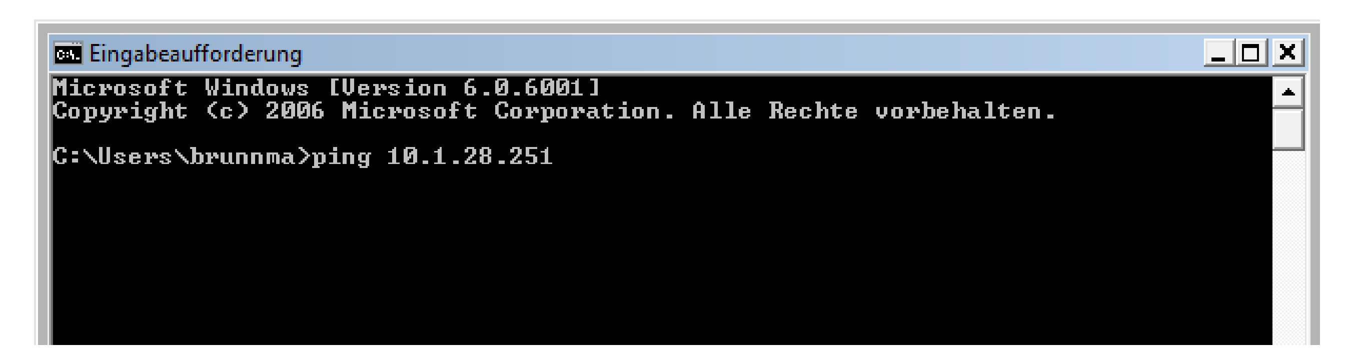


5.2.3.4 Überprüfen der ekey net CV LAN Funktion im Netzwerk

5.2.3.4.1 PING

Nachdem Sie den ekey net CV LANfertig konfiguriert haben, können Sie die Erreichbarkeit im Netzwerk abprüfen. Starten Sie unter

Windows -> alle Programme -> Zubehör ->Eingabeaufforderung



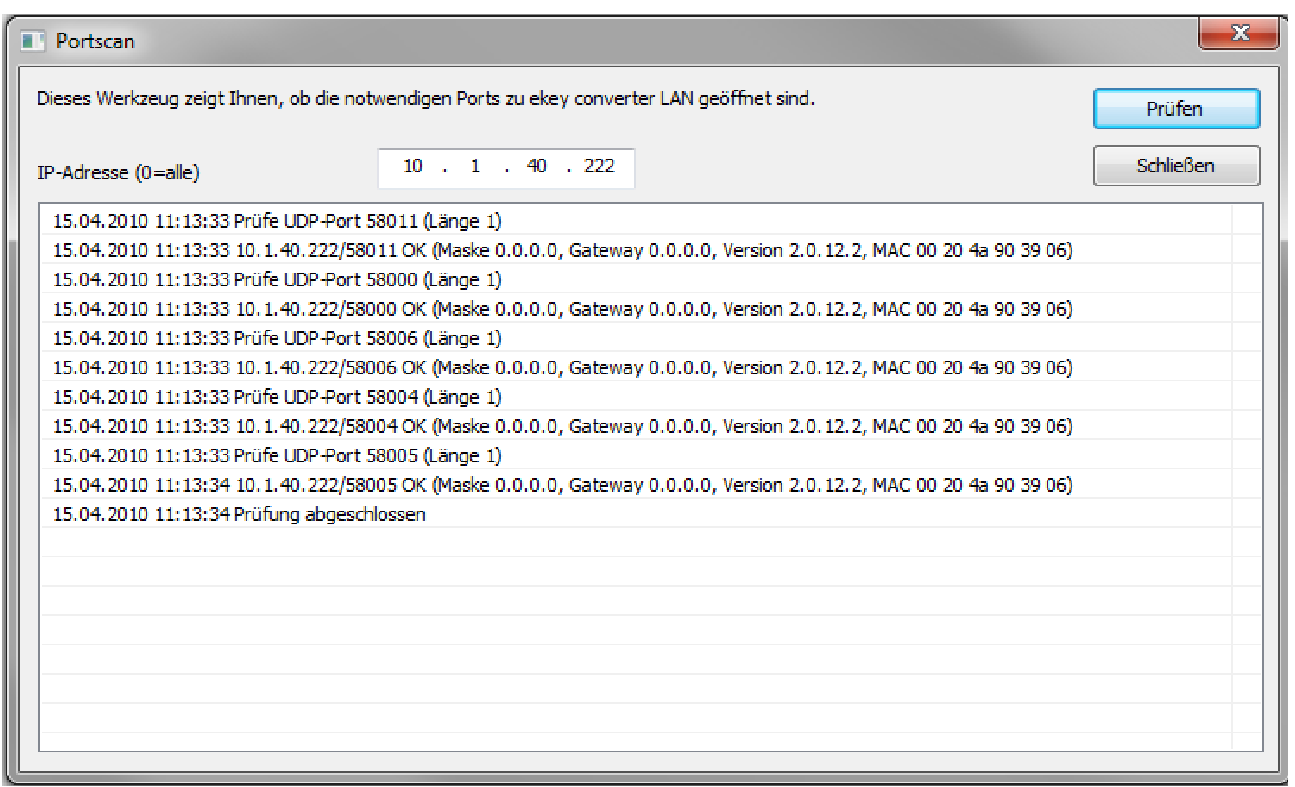
und machen Sie einen „Ping" auf die IP-Adresse (z.B. Ping 10.1.28.251) des ekey converter LAN. Erhalten Sie entsprechende Antworten ist die Funktion und die Netzwerkverbindung zum ekey net CV LAN von diesem Rechner (PC, Server) aus in Ordnung.

5.2.3.4.2 Portscan

Ihre ekey net CV LAN funktionieren im ekey net nur einwandfrei, wenn die entsprechenden Kommunikationsports vom ekey net Terminalserver zum ekey net CV LAN frei sind. Im Programm ekey net CV LAN config können Sie prüfen, ob ihr Netzwerk diese Kommunikation zuläßt.

Klicken Sie dazu, nachdem Sie einen ekey net CV LAN aus der Liste gewählt haben,auf Portscan... .
Es erscheint dann folgendes Fenster:





Alle geprüften Portnummernmüssenein OK liefern!

5.2.3.4.3 FAQ ekey net LAN Converter wird nicht gefunden

Öffen Sie das Programm **ekey CONVERTER LAN CONFIG**

Info: ekey net CV LAN haben im Auslieferungszustand die IP Adresse 192.168.1.250

Falls Ihr Netzwerk andere IP Adressen verwendet (anderes Subnetz) können Sie den CV LAN über den Button „Manuelle Auswahl" suchen oder er erscheint trotzdem da er über ein MAC-Adressen-Broadcast gefunden wird.
Dies kann von diversen Router oder Layer 3 Switches aber geblockt werden.

- IP Adresse des Converters muss statisch sein (kein DHCP)
- Firewall/Router lässt keinen Broadcast zu.
  --> Firewall abdrehen
- Firewall/Router hat keine Ausnahme (Ports 58000-58018 sind nicht eingetragen).
  --> Firewall abdrehen bzw. Ausnahmen setzen
- Ports sind von einem anderen Programm reserviert.
  --> Portscanner runterladen damit man sehen kann welche UDP-Ports von welchem Programm benötigt werden (z.B TCP View von Sysinternal)
- Testen über MS-DOS Eingabeaufforderung ob pingbar

- Wenn der PC im selben Subnetz wie der Converter ist und nicht pingbar ist.
  --> die beiden Leds beim Converter beobachten
    --> wenn beide nicht leuchten Stromproblem
    → beide LED blinkt orange -> Firmwarefehler
    --> links ist Power LED rechts activity LED
  --> Converter Stromreset machen.
  --> evtl. auch beim Switch einmal Stromreset.
- Sollte der CV LAN weiterhin nicht erscheinen, versuchen Sie über den Button „IP zuweisen / Reset Converter" dem LAN Converter über die manuelle Eingabe der MAC Adresse eine NEUE und ANDERE IP zu geben bzw. über „Manuelle Auswahl…" suchen.
- „Nur für Analyse" darf im ConverterLanConfig nicht angehackt sein
- Wenn die eigene IP Adresse (zb. am Notebook) geändert wurde, muss der Communication-Dienst neu gestartet werden

Prüfen Sie ob alle ekey Dienste laufen und Message Queuing

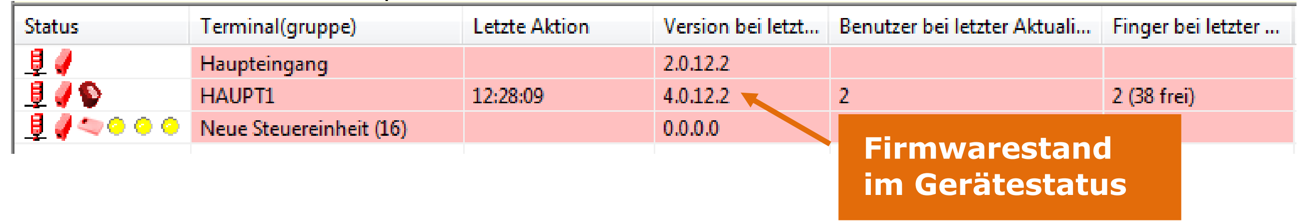
5.2.4 ModulUpdate

Vor allem beim Update von einer älteren Version von ekey net aber auch bei einer Neuinstallation ist als erster Schritt unbedingt zu prüfen, inwieweit die Firmwarestände auf den Geräten

- ekey net FS
- ekey net SE
- ekey net CV LAN

dem aktuellen Stand entsprechen. Unter Umständen ist ein Update notwendig. Die Firmwarestände der in Betrieb befindlichen Geräte können Sie einerseits im Gerätestatus ablesen, und mit den im Readme.txt gelisteten Ständen vergleichen. Sie sehen dann welche Geräte Sie updaten müssen.Alternativ dazu können Sie gleich das Programmstarten.

Ein ModulUpdate können Sie erst nach Durchführung der ekey net CV LAN – Konfiguration machen. Sehen Sie dazu Kapitel 5.2.3.2



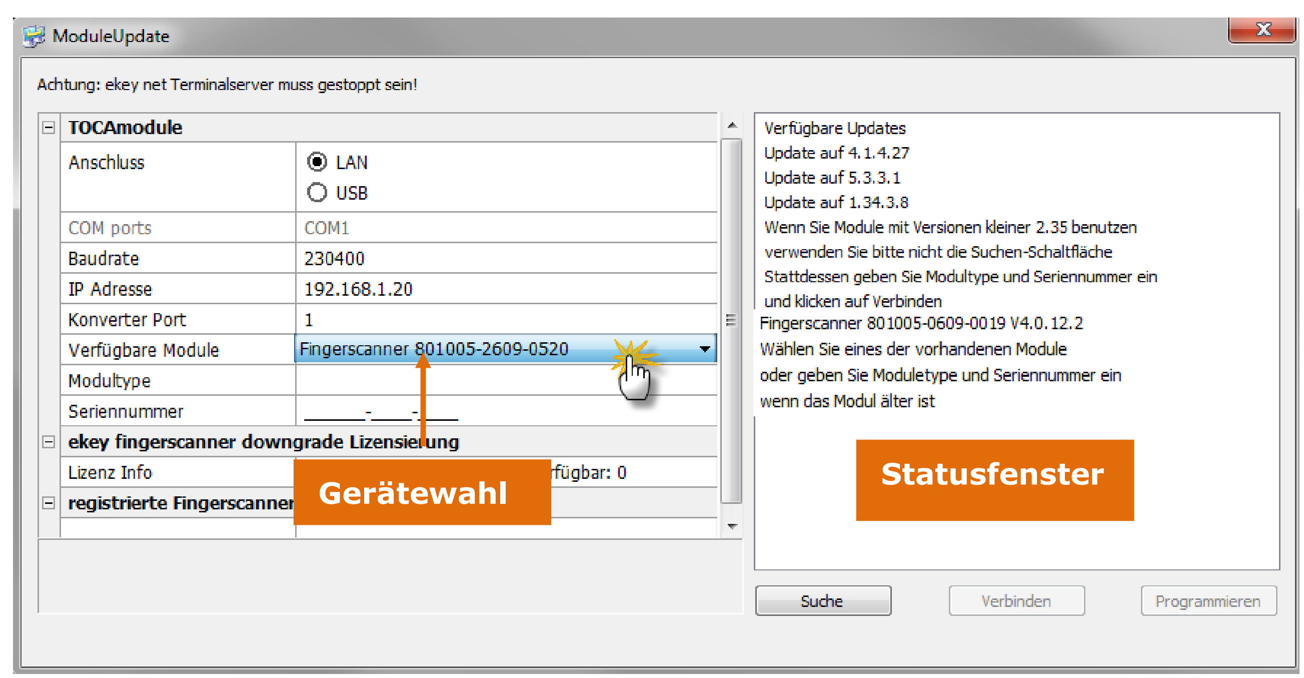
Status	Terminal(gruppe)	Letzte Aktion	Version bei letzt...	Benutzer bei letzter Aktuali...	Finger bei letzter ...
	Haupteingang		2.0.12.2		
	HAUPT1	12:28:09	4.0.12.2	2	2 (38 frei)
	Neue Steuereinheit (16)		0.0.0.0		

© 2010 – ekey biometric systems GmbH





Vor einem ModulUpdate** stellen Sie noch sicher, dass die im System laufenden Dienste **ekey Service Guard und ekey net Terminalserver** beendet (gestoppt) sind! **ekey ModulUpdate funktioniert ansonsten nicht.

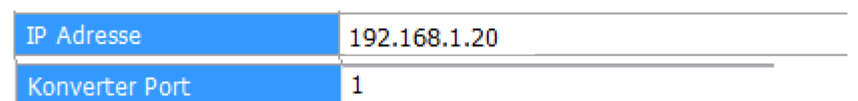


Im Statusfenster sehen Sie nun die letztgültigen Programmversionen gelistet. In diesem Beispiel:
Update auf 4.1.4.27(Fingerscanner)
Update auf 5.3.3.1 (Fingerscanner)
Update auf 1.34.3.8(Steuereinheit)

Beginnen Sie nun bei der Prüfung der Einstellungen

Anschluß	◉ LAN ○ USB
COM ports	COM4
Baudrate	230400

Normalerweise sind die Werte „**Anschluss**" und „**Baudrate**" bereits fix eingestellt. Sehen Sie hier anderes, ändern Sie es auf LAN bzw. 230400



IP Adresse	192.168.1.20
Konverter Port	1

Geben Sie nun die IP-Adresse und den Konverter Port (immer „1") des ersten ekey converter LAN ein und klicken Sie auf Suche



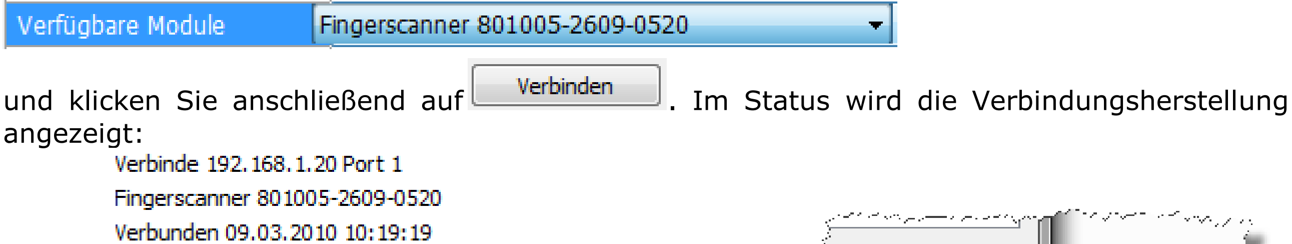
Damit Sie mit dem ekey net CV LAN eine Verbindung herstellen können, muss dieser netzwerktechnisch von dem PC auf dem das Programm ModulUpdate läuft, erreichbar sein, d.h. er muss im selben Netz liegen!

ModulUpdate listet nun alle Geräte die mit diesemekey net CV LANverbunden sind.

Verbinde 192.168.1.20 Port 1
Fingerscanner 801005-2609-0520 V4.1.6.3
Steuereinheit 800340-1706-0032 V1.33.11.25
Wählen Sie eines der vorhandenen Module
oder geben Sie Moduletype und Seriennummer ein
wenn das Modul älter ist

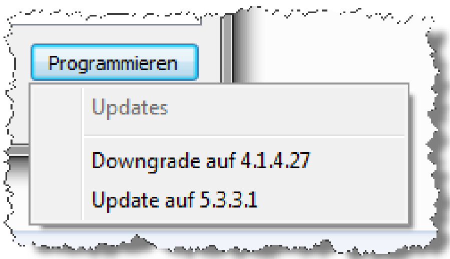
In unserem Beispiel findet ModulUpdate den Fingerscanner mit der Seriennummer 801005-2609-0520. Die Programmversion auf dem Fingerscanner ist 4.1.6.3und damit alt (die Neue ist 5.3.3.1). Es ist also ein Update erforderlich.

Wählen Sie nun in der Combobox „**verfügbare Module**" jenen Fingerscanner aus, den Sie updaten möchten



und klicken Sie anschließend auf [Verbinden]. Im Status wird die Verbindungsherstellung angezeigt:

Verbinde 192.168.1.20 Port 1
Fingerscanner 801005-2609-0520
Verbunden 09.03.2010 10:19:19
Version 4.1.6.3
Bereit zum Modulupdate
Downgrade auf 4.1.4.27
Update auf 5.3.3.1



Klicken Sie nun auf [Programmieren] und wählen Sie **Update**.

Das Update des gewählten Gerätes beginnt. Sie sehen unterhalb des Programmfensters einen Fortschrittsbalken.

Geräteaktualisierung 20%

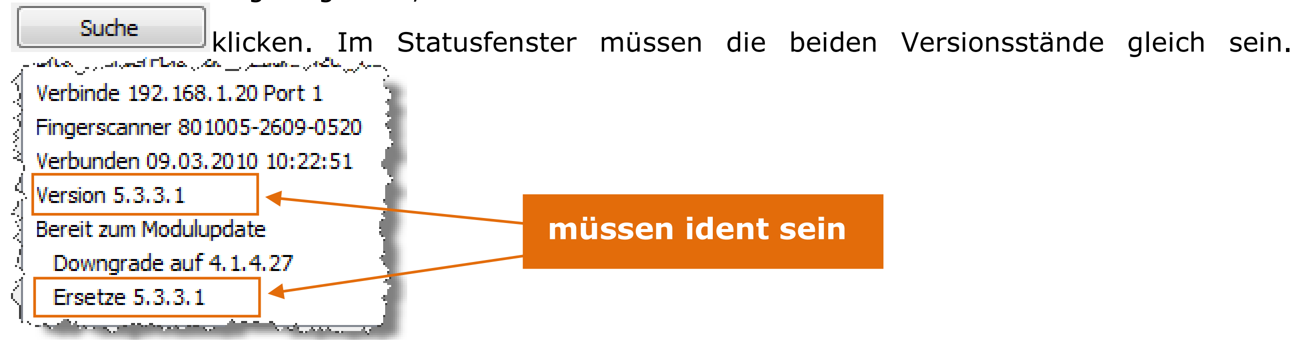
Nach dem die Aktualisierung abgeschlossen ist, erscheint im Statusfenster die Meldung

Bitte warten bis das Module neu gestartet hat!

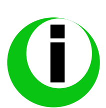
Warten Sie hier unbedingt bis der Fingerscanner (FS) oder Steuereinheit (SE) wieder durchstarten. -> grüner Pfeil leuchtet (bei FS) bzw. rote Punkte leuchten oder blinken(bei SE). Dies dauert nach Abschluss der Aktalisierung ca. 30 sek – 1min.

STOP **Unterbrechen Sie während dieser Zeit auf keinen Fall die Stromversorgung. Dies kannzu einem Firmwaredefekt des Gerätes führen, der unter Umständen nur im Werk wieder behoben werden kann.**

Prüfen Sie dann, nachdem das Gerät wieder durchgestartet hat, ob nun der aktuelle Firmwarestand angezeigt wird, indem Sie nochmals auf



klicken. Im Statusfenster müssen die beiden Versionsstände gleich sein.



Es kann vorkommen, dass ein Update durch
- *Netzunterbrechungen*
- *Übertragungsfehler*

misslingt. Wiederholen Sie einfach den Vorgang nochmals. Sie können das auch mehrmals versuchen.

5.2.5 Abschluss der Installation

Vergessen Sie nachdem Sie die Installation abgeschlossen haben nicht die Lizenzpakete für Ihre ekey net FS bei ekey zu aktivieren. Gehen Sie dazu nach Kapitel 3.5.2 vor.



Für die Aktivierung der Lizenzen haben Sie 30 Tage Zeit. Details zur Aktivierung finden Sie im Kapitel 3.5.2. Wenn die Aktivierung nicht erfolgt, so schaltet das System in den Offline-Modus und Sie können keine Konfigurationsänderungen durchführen.

5.3 Update von Vorgängerversionen ekey net

5.3.1 Allgemein



Vorbereitung des Updates:
- **Sicherheitshalber sollten Sie die Datenbank– Datei („TOCAnet.netdata" – „ekey net.netdata" ab Version 4.0) aus dem Datenbank-Ordner von ekey net wegsichern. Falls es während der Installation zu einem Crash kommt, gehen somit die Finger und Benutzerdaten nicht verloren!!**
- Prüfen Sie die Installationspfade! Diese müssen denen der Erstinstallation entsprechen. ekey net wird ansonsten ein zweites Mal installiert, was zu massiven Fehlfunktionen führen kann! (Siehe Kapitel 5.2.2)

5.3.2 Lizenzen

Haben Sie bereits eine ekey net Version vor ekey net 3.5 in Betrieb und Sie möchten auf die Version 3.5 oder höher updaten, **so müssen Sie im ersten Schritt die notwendige Anzahl an ekey net Lizenzen ermitteln**. Ein Update auf 3.5 ist erst möglich, wenn Sie die notwendige Anzahl an ekey net Lizenzen von ekey erhalten haben, und diese im ekey LizenzManager gelistet sind**.**



Für die Aktivierung der Lizenzen haben Sie 30 Tage Zeit. Details zur Aktivierung finden Sie im Kapitel 3.5.2. Wenn die Aktivierung nicht erfolgt, so schaltet das System in den Offline-Modus und Sie können keine Konfigurationsänderungen durchführen.



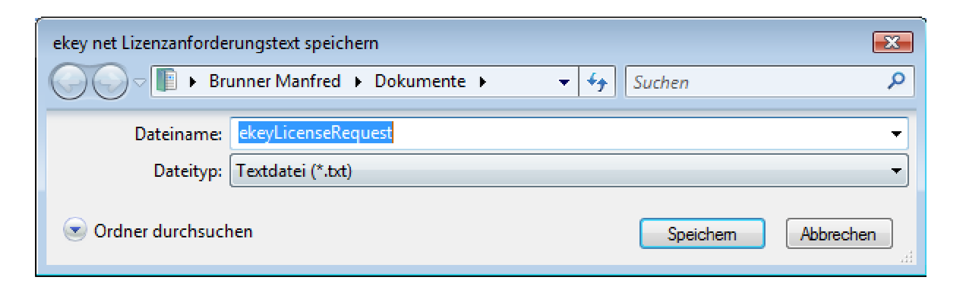
Verwenden Sie zur Überprüfung der nötigen Lizenzen das Programm ekeyNetUpdateCheck.exe
Sie finden dieses Tool auf der ekey net CD unter „**checkUpdate**".
Kopieren Sie die Datei in das Programmverzeichnis von ekey net auf dem Rechner/Server, auf dem der ***ekey net Masterserver*** arbeitet. Starten Sie das Programm

Das Tool ermittelt die Anzahl der für den Betrieb der ekey net FS fehlenden Lizenzen in Ihrem System und kreiert einen Key, den Sie per Email anlicense@ekey.net senden.



Es werden nur Fingerscanner erfasst, welche in der aktuellen Datenbank konfiguriert sind und mindestens einmal im Onlinezustand waren!

Der Key wird in die DateiekeyLicenseRequest.txt gespeichert, welche Sie an einem passenden Ort ablegen können.



Transferieren Sie diese Datei dann auf einen Rechner von dem Sie ein Email absenden können und senden Sie ein E-Mail mit dieser Datei als Anhang an***license@ekey.net***

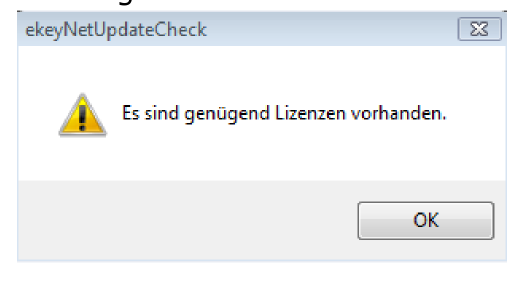
Sie erhalten dann nach maximal 2 Werktagen eine Datei **(.kfu)** per Email retour. Diese Datei beinhaltet die Lizenzen für das Update.



Ohne diese Datei kann das Update NICHT durchgeführt werden. Die Eingabe von Lizenz-Keys ist bei einem Update NICHT möglich. Es muss die „.kfu" Datei eingespielt werden!



Haben Sie bereits genug Lizenzen aktiviert, so erscheint folgende Message-Box:



Sie können nun mit dem Update beginnen.

5.3.3 Setup

Starten Sie nun das ekey net Setup (Setup.exe)

Danach startet der ekey net InstallShield Wizard



Bestätigen Sie hier mit Weiter>

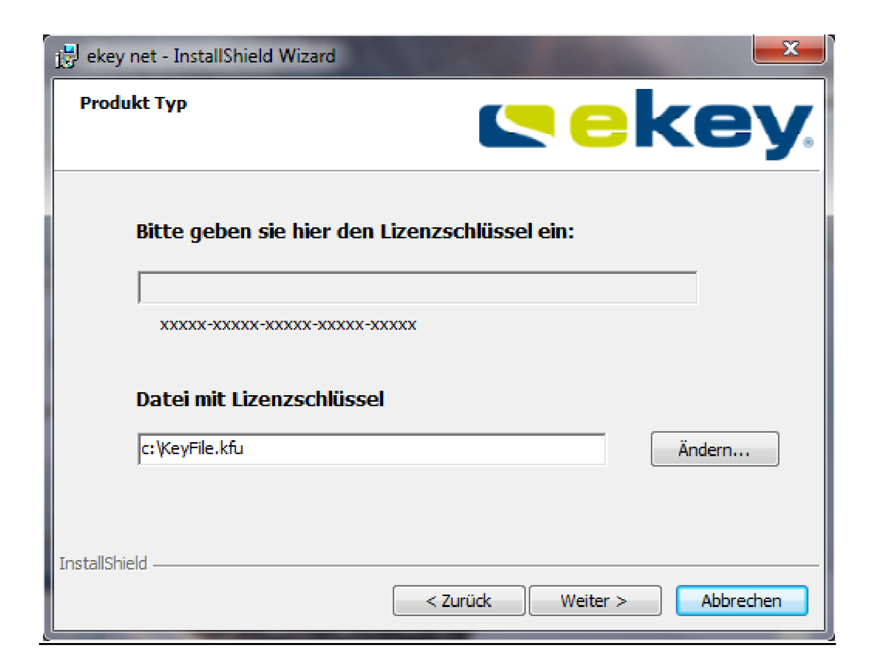
Es öffnet sich das Fenster mit dem Lizenzvertrag. Bitte lesen Sie diesen sorgfältig durch und bestätigen Sie durch Auswahl des Feldes

Ich akzeptiere die Bedingungen der Lizenzvereinbarung

und anschließenden Klick auf Weiter>







Lesen Sie nun die zuvor von ekey erhaltene **.kfu-Datei** ein. Mit „**Ändern**" können Sie die Datei entsprechend wählen und klicken Sie dann auf weiter.

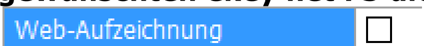
- Gehen Sie nun weiter ident zu Kapitel 5.2.2 vor.
- Als nächstes bringen Sie die **ekey net CV LAN** (siehe Kapitel 5.2.3.3) unddie **ekey net Geräte (Fingerscanner, SE,…)** mit dem Programm **ModulUpdate** (siehe Kapitel5.2.4)auf den letzten Firmwarestand.
- Abschließend aktivieren Sie noch die ekey net Lizenzen (siehe Kapitel 3.5.2)



Für die Aktivierung der Lizenzen haben Sie 30 Tage Zeit. Details zur Aktivierung finden Sie im Kapitel 3.5.2. Wenn die Aktivierung nicht erfolgt, so schaltet das System in den Offline-Modus und Sie können keine Konfigurationsänderungen durchführen.

5.3.4 Konfigurationsänderungen durch das Update

Wenn Sie mit der Funktion Web-Logging arbeiten, so aktivieren Sie noch bei den gewünschten ekey net FS die Funktion Web-Aufzeichnung:



Siehe Kapitel 6.6.3.2.3.2

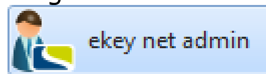


Nach einem Update von ekey net 3.x auf ekey net 4.x müssen Sie die Web-Aufzeichnung an den genwünschten ekey net FS aktivieren In den Vorgängerversionen wurde automatisch von allen ekey net FS aufgezeichnet.

6 Konfiguration und Administration des Systems

6.1 ekey net AdminStartfenster

Alle Einstellungen und Parametrierungen im ekey net werden im ekey net Admin vorgenommen. Starten Sie dazu aus dem Windows – Programmverzeichnis das Programm





Geben Sie in das Textfeld „**Server**" den **Namen** des Computers ein, auf dem der ekey netMasterserver installiert wurde.



Ihre Netzwerkkonfiguration muss es zulassen, dass die Server gegenseitig bidirektional über Servernamen erreichbar(pingbar) sind (DNS)

Die Anmeldedaten für das Standard-Administratorkontolauten:

Administrator: **Administrator**
Kennwort: **admin**

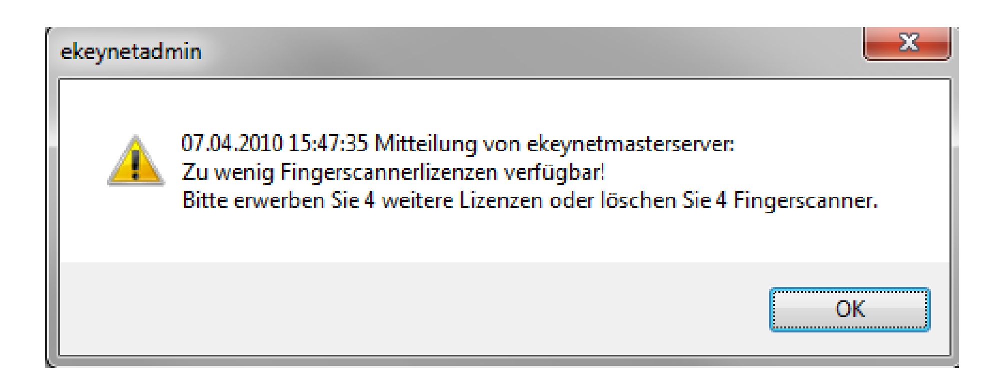
Später können hier dann die Administratoren mit ihrer**Benutzer - Bezeichnung** -> „**Vorname Nachname**", **„Nachname Vorname"**, **„Nachname, Vorname"** od. **„frei definiert"**und dem erstelltenPasswort ->**siehe Kapitel 8.1.5.1**den ekey net Admin starten



BITTE beachten Sie bei der Eingabe die Groß- und Kleinschreibung. Achten Sie weiters auf die Möglichkeit, dass das Feld „Bezeichnung" eventuell verändert wurde
-> Kapitel 6.4.2.2

Nach Bestätigung durch Klick auf die Taste „**Anmelden**" öffnet sich der ekey net Admin.





Der ekey net Admin prüft nach seinem Start die aktivierte Lizenzanzahl zur Anzahl der registrierten Fingerscanner im ekey net. Sind zu wenige Lizenzen aktiviert, so wird dies mit obiger Message-Box gemeldet. Damit Sie hier nun weiter fortfahren können, aktivieren Sie die noch offene Anzahl von Lizenzen.



Betreiben Sie ekey net nach dieser Meldung ohne Korrektur, so funktioniert die Anzahl von ekey net FS ohne Lizenz nicht ordnungsgemäß. Welche Scanner innerhalb von ekey net davon aber betroffen sein werden, kann nicht gesagt werden!

Startbild des ekey net Admin

LIGHT

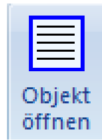
BUSINESS **COM**

Grundsätzlich haben Sie 6 Konfigurationsbereiche in ekey net. Die Menüs können sich im Umfang der Einstellungsmöglichkeiten je nach ekey net Version LIGHT COM BUSINESS unterscheiden

- START
- DATEN
- BENUTZERBERECHTIGUNG
- TERMINALS
- STATUS
- GRUNDEINSTELLUNGEN

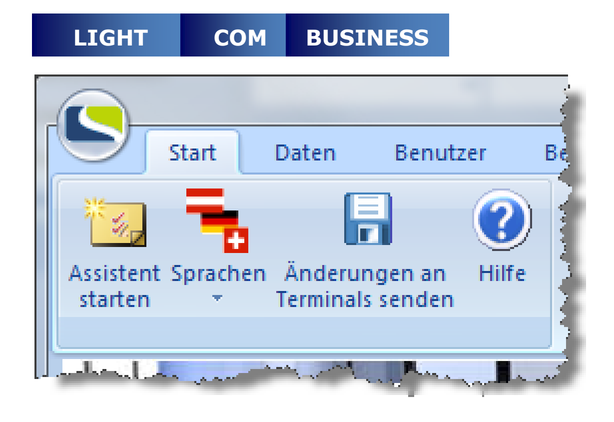


Änderungen der Objekte in diesen Bereichen werden grundsätzlich immer mit dem Assistenten durchgeführt. Mit der Funktion **Objekt öffnen** wird dieser passend zum entsprechenden Objekt gestartet.



6.2 Menü „START“

LIGHT COM BUSINESS

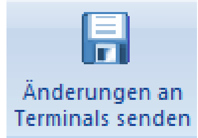




Der Assistent startet automatisch beim erstmaligen Aufruf von ekey net Admin bzw. wenn noch keine Eingaben (Konfigurationen) gemacht wurden. Sie können ihn aber auch im Menü „**Start**“ jederzeit mit einem Klick starten.Details zum Assistenten folgen im Kapitel**7„Der Assistent“**



Der Wechsel auf alle verfügbaren Sprachen kann jederzeit in Echtzeit erfolgen. Die verfügbaren Sprachen können Versionsbedingt variieren und werden laufend erweitert.



Nach Änderungen der Konfigurationseinstellungen können Sie damit diese an das System übergeben
Erst damit werden die Änderungen und Einstellungen im System aktiv!!

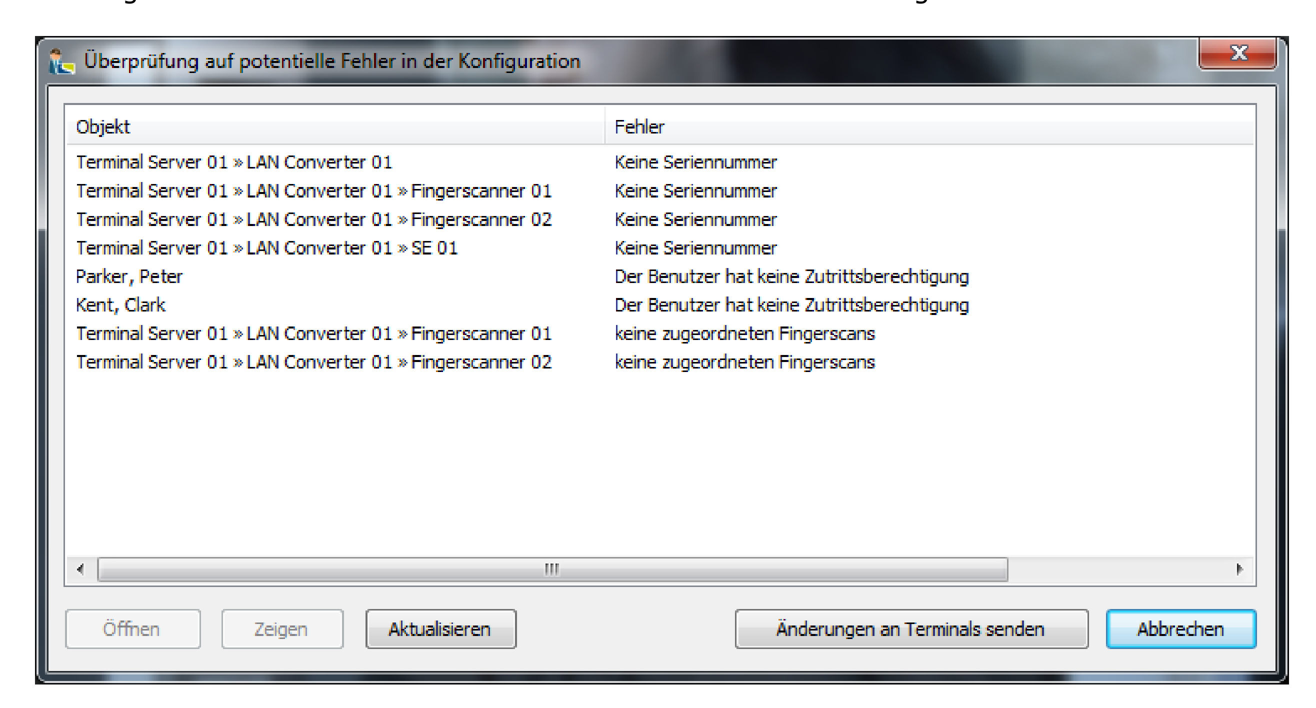


Über die Schaltfläche Hilfe können Sie jederzeit dieses Dokument öffnen



Ab Version ekey net 4.1 werden potentiell Fehler in der Konfiguration und Statusinformationen beim „Änderung an Terminals senden“ als Dialog gemeldet.

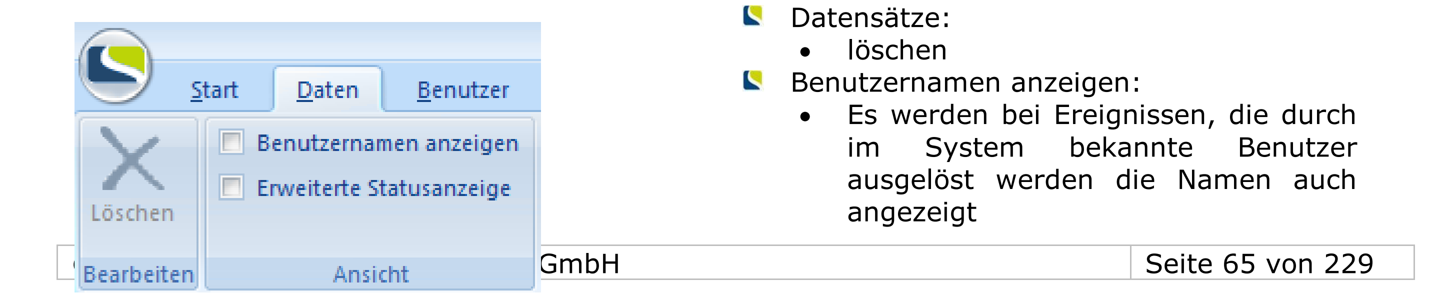
folgende Checks sind vorhanden:
Computernamen von Terminalservern mehrfach verwendet
IP Adressen von ekey Converter LAN mehrfach verwendet
Seriennummern von FS, SE oder ekey Converter LAN ist 0
Seriennummern von FS, SE oder ekey Converter LAN mehrfach verwendet
aktive Benutzer ohne Zugangsberechtigung
zu alte Firmware bei FS und SE
keine Finger auf Fingerscanner
zu viele Finger auf FIngerscanner
Fingerscanner Hardware V5 (Atmel) und V6 (Authentec) gemischt auf CV LAN
Prüfung ob FAR vorhanden ist
Prüfung ob Default Kennwort von TOCAadmin bzw. Admnistrator geändert wurde



6.3 Menü „DATEN“

6.3.1 Funktionen und Inhalte im Datenfenster

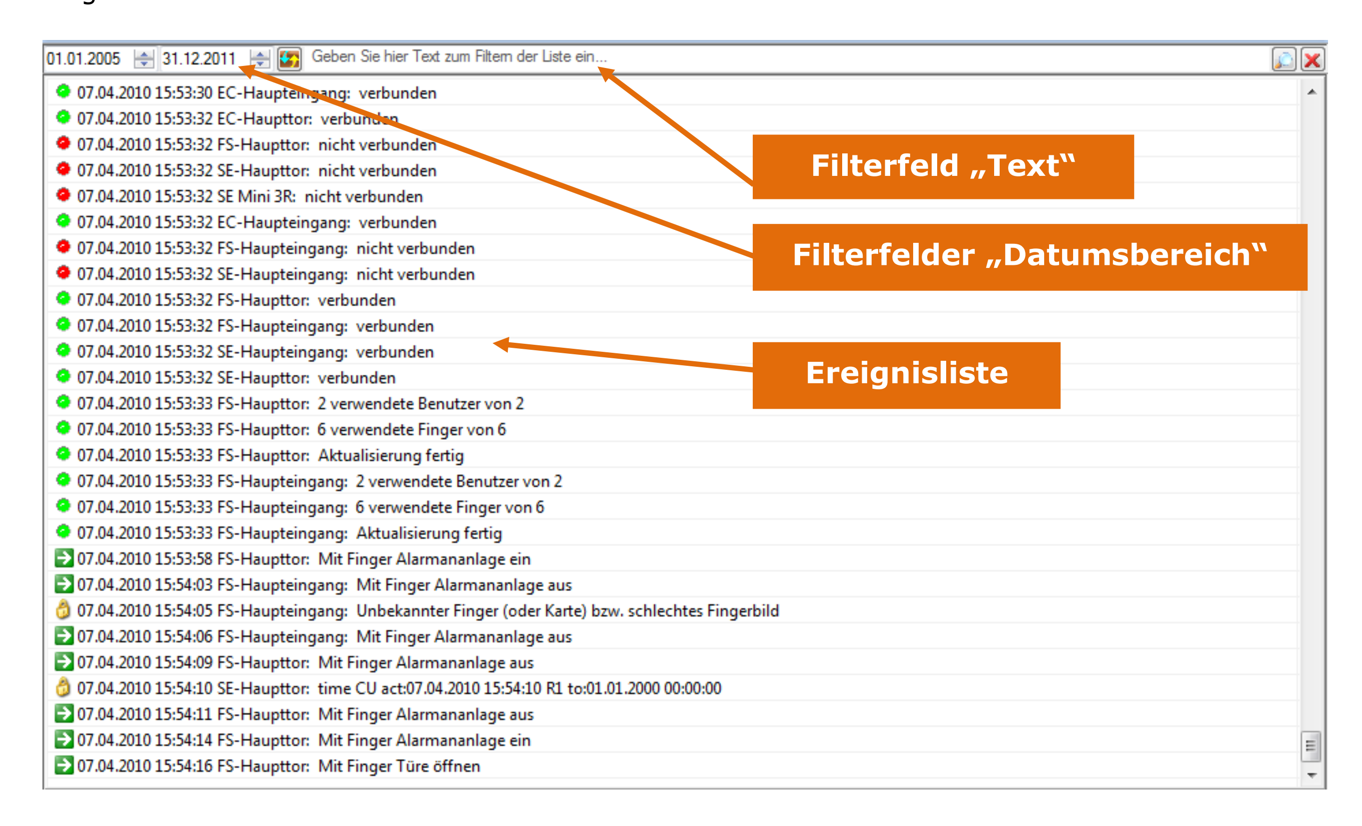
Über die Symbolleiste des Menüs „Daten“ können Sie folgende Auswahl treffen:



- Datensätze:
  - löschen
- Benutzernamen anzeigen:
  - Es werden bei Ereignissen, die durch im System bekannte Benutzer ausgelöst werden die Namen auch angezeigt

- Erweiterte Statusanzeige aktivieren:
  - Es werden in der Ereignisliste auch die Systemmeldungen angezeigt

Sie können hier also nachprüfen, welche Ereignisse in der Vergangenheit im System ekey net aufgetreten sind.

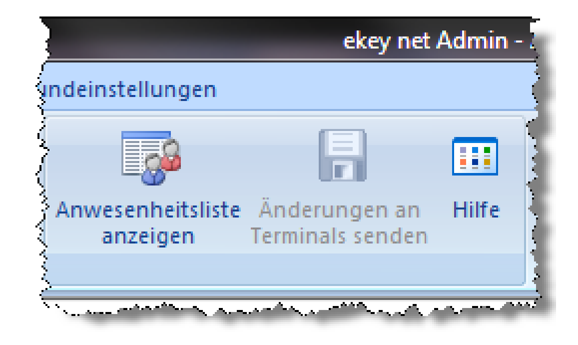


Im obigen Statusfenster sieht man beispielhaft eine Ereignisliste.Jeder Logeintrag ist mit Datum und Uhrzeit versehen und die Einträge sind chronologisch gereiht.

Sie können diese Liste nun in der
- Ansicht ändern
- bearbeiten

indem Sie das entsprechende Symbol aus der Symbolleiste wählen.

Mit „**Löschen**" löschen Sie die gesamte Liste im ekey net.



- Anwesenheitsliste:
  - Damit öffnen Sie die Anwesenheitsliste – Details dazu im Kapitel 10
- Änderungen an Terminal senden:
  - Möglichkeit zur Aktualisierung des Systems
- Hilfe:
  - Öffnen Sie dieses Handbuch als PDF

6.3.2 Berichte über Benutzer- oder Fingerscanneraktivitäten



Diese Funktion ist nur aktiv, wenn die „Berichtwesen" in den „Grundeinstellungen –> Aufzeichnung" aktiviert und ordnungsgemäß konfiguriert ist. Siehe Kapitel 15.1.8

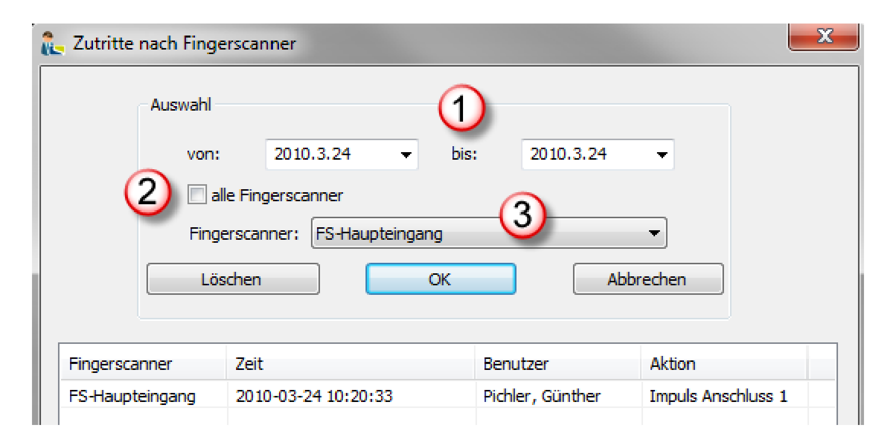


Ab der ekey net Version 4 ist es einfach möglich folgende Berichte:

- Am Bildschirm an zu zeigen
- Als HTML zu exportieren -> anschließende Druckmöglichkeit aus dem WEB-Browser
- Als CSV-Datei zu exportieren



6.3.2.1 Zutritt nach Fingerscanner:

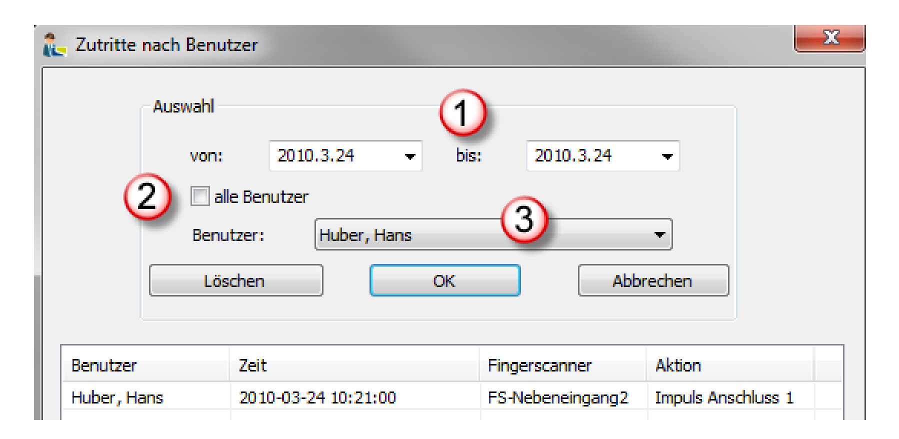


1 Wählen den gewünschten Datumsbereich – von: -> bis:

2 Für die Auswahl aller Fingerscanner aktivieren Sie die Checkbox

3 oder wählen Sie gezielt einen bestimmten Fingerscanner aus

6.3.2.2 Zutritt nach Benutzer



1 Wählen den gewünschten Datumsbereich – von: -> bis:

2 Für die Auswahl aller Benutzer aktivieren Sie die Checkbox

3 oder wählen Sie gezielt einen bestimmten Benutzer aus

Die angezeigten Berichte können Sie nun exportieren oder als HTML speichern, um die Daten in weiterer Folge in einem WEB-Browser an zu zeigen oder aus zu drucken.



6.3.3 Datenfenster im Gerätestatus

Um zum Gerätestatus zu kommen klicken Sie aufdas Menü **Status.**

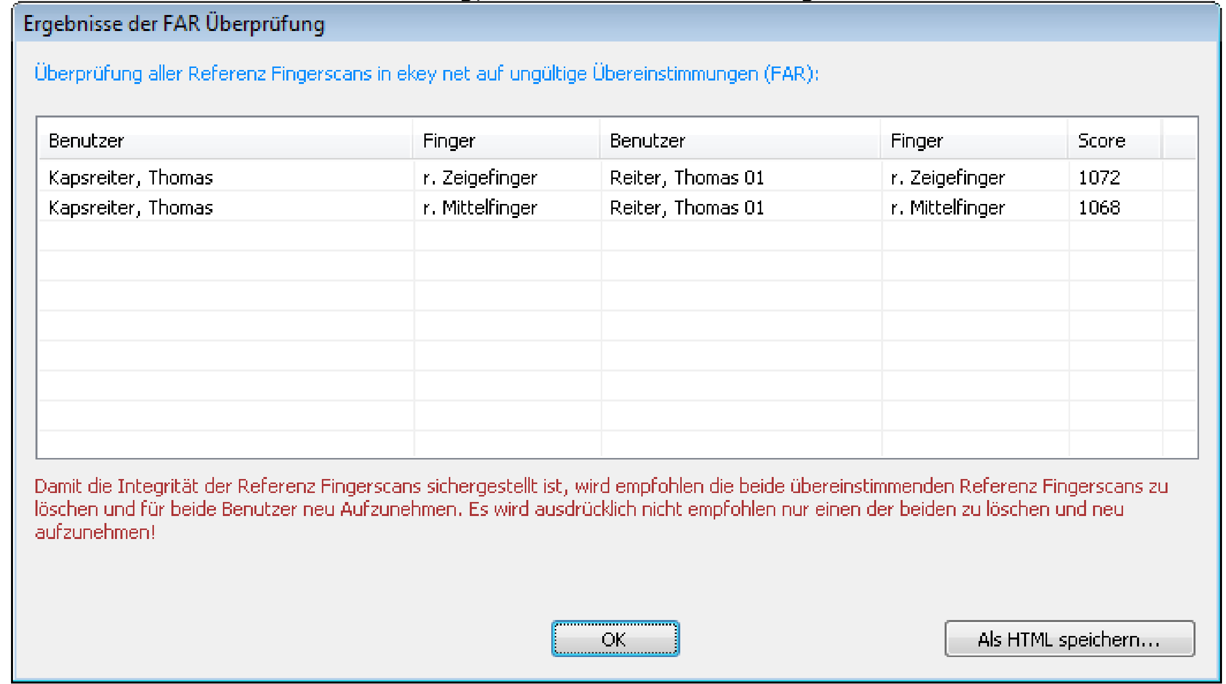
Klicken Sie dort auf ein spezifisches Gerät oder eine Gerätegruppe, so sehen Sie nur die Log-Einträge die dem Gerät bzw. der Gerätegruppe zugeordnet sind. Ansonsten sind „**Benutzernamen anzeigen**" und „**erweiterte Statusanzeige**" genau so über das Pop-Up Menü erreichbar wie unter Kapitel6.3.1 beschrieben.

6.3.4 FAR-Check

Ab Version ekey net 4.1 können Sie einen FAR-Check durchführen.
FAR=Falschakzeptanzrate
Das System überprüft ob es 2 Benutzer gibt die gleiche Finger haben, dies kann vorkommen wenn versehentlich eine Person 2 mal angelegt wurde oder die Finger von 2 unterschiedlichen Personen falsch aufegnommen wurden (zb. nur Fingerkuppe)



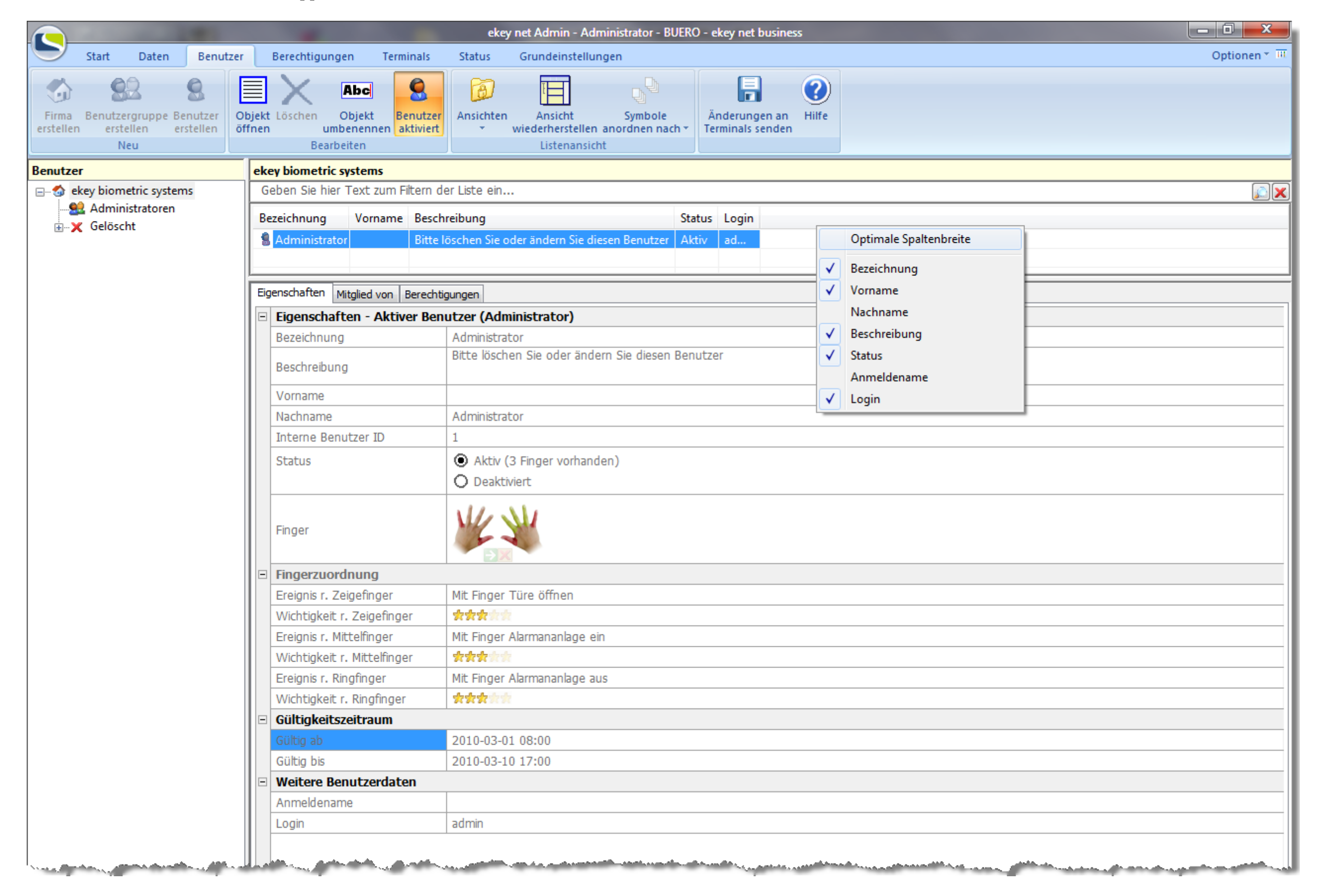
Klicken Sie rechts auf FAR Prüfung, falls ein Problem vorliegt erscheint ein Informationsfenster.



Sie sehen dann welche beiden User/Finger im System gleich sind und können dies korrigieren.



6.4 Menü „BENUTZER"



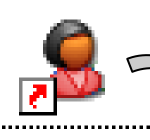
Die Eingabe der Daten auf BENUTZEREBENE umfasst

- Benutzergruppen
- benutzerspezifische Daten (Name usw.)
- Fingeraufnahme
- RFID- Kartennummer
- Ereigniszuweisung

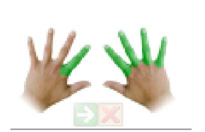
Im Menü „BENUTZER" definieren Sie die Benutzerdaten, sowieFinger(Finger der Personen werden aufgenommen) und Medien (RFID) und Sie weisen jedem dieser einzelnen Fingeroder Medien ein Ereignis zu. Damit sind die Benutzer selbst und auch die dazugehörigen Finger samt der Funktionalität im System bekannt.



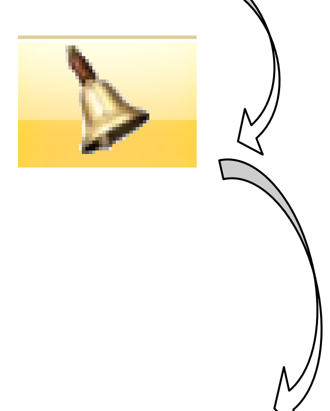
6.4.1 Schematischer Ablauf der Benutzeranlage



Benutzerdaten werden erfasst (Name, Position usw.)



die **Finger bzw. Medium (Karte)** des Benutzers werden aufgenommen.



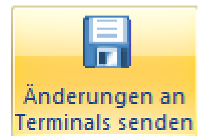
Den einzelnen **Fingern** werden **Ereignisse** zugewiesen
Ein Finger -> Ein Ereignis



Hinweis zur Wirkung dieser Zuweisung:

Ein ausgelöstes Ereignis führt wiederum zu einer Aktion. Eine Aktion ist beispielsweise das Schalten eines Relais auf einer ekey net SE. Im ekey net Admin können
einem Ereignis **eine (zwei)** Aktion(en)
zugeordnet werden.

Die Aktion(en) werden dann auf einer Steuereinheit entsprechend ausgeführt (z.B. Schalten von Relais 1 für 3 Sekunden).



Änderungen an Terminal senden durchführen. **Damit wird die Änderung im System erst aktiv!!**



*In dieser Ebene ist **NICHT** bekannt,*
- *auf welcher Steuereinheit im System die Aktion ausgeführt werden soll*
- *ob überhaupt eine Berechtigung zum Ausführen der Aktion vorliegt (örtliche / zeitliche / kalendarische Berechtigung).*

*Deshalb erfolgt noch keine Aktionsausführung im System, ohne die entsprechenden Konfigurationen von **TERMINAL**- und **BERECHTIGUNGSEBENE**.*

6.4.2 Eingabe der Parameter und Daten

6.4.2.1 Firmen und Benutzergruppen



Im ekey net können Sie um,
- eine bessere Systemübersicht über ihre Benutzer
- eine einfachere und übersichtliche Berechtigungsstruktur

zu haben, Firmen und/oder Benutzergruppen anlegen.
Die Anlage erfolgt im Menüreiter„Benutzer"



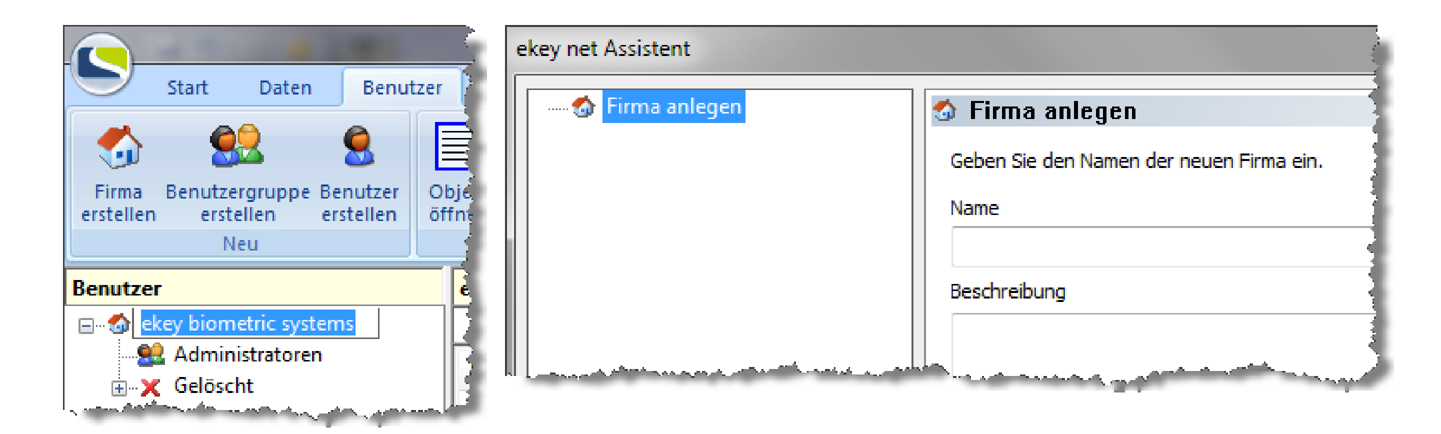
Firmen sind getrennte Organisationseinheiten. Benutzer aus einer Firma können grundsätzlich nur Berechtigungen innerhalb dieser Firma erhalten. Zwischen unterschiedlichen Benutzergruppen innerhalb einer Firma können die Berechtigungen jedoch variieren.

© 2010 – ekey biometric systems GmbH



Bevor Sie mit der Benutzerkonfiguration beginnen, überlegen Sie genau welche Benutzer gleiche Rechte (gleiche Zeitfenster des Zutritts) haben, und fassen Sie diese zu Gruppen zusammen. Die Übersichtlichkeit des Systems, die Vereinfachung der Wartung und damit letztlich die Betriebssicherheit wird sich enorm erhöhen. Sie sparen dadurch Zeit und Geld!

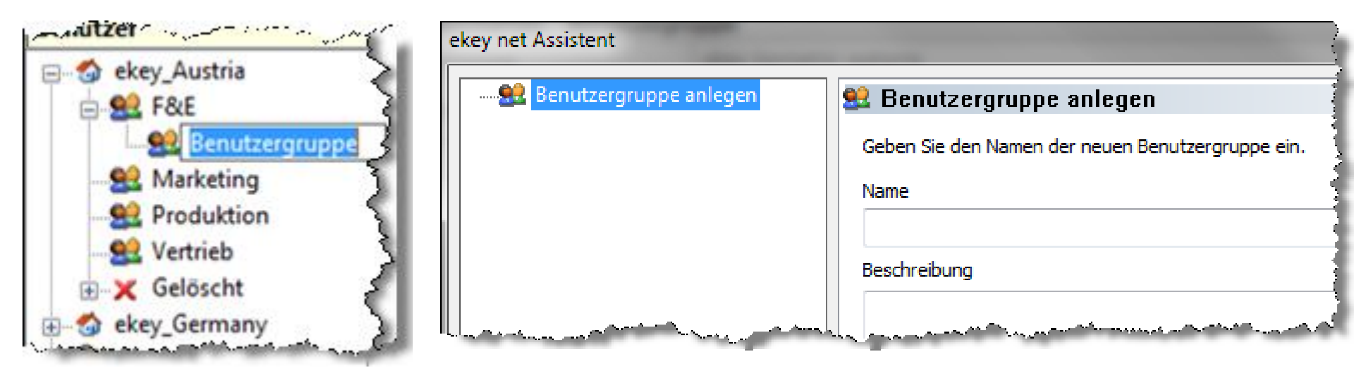
Durch Klick auf den Menü-Button **„Firma erstellen"** legen Sie die obersten Ebenen fest. So können Sie z.B. Filialbetriebe klar erkennen.



Im ekey net Assistenten definieren Sie den„**Namen**" der Firma. Des Weiteren können noch Zusatzinformationen unter „**Beschreibung**" eingetragen werden.



Bei Klick auf denButton „**Benutzergruppe erstellen**" legen Sie nun Benutzergruppen an.

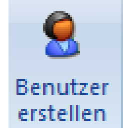


Benutzergruppen dienen der Übersichtlichkeit des Systems und der einfacheren Verwaltung. Es liegt an Ihnen wie Sie die Gruppen aufbauen. Sie können hier auch mehrere Ebenen (praktisch unbegrenzt) aufbauen.
Wir empfehlen Benutzer mit gleichen Rechten (Zeit des Zutritts am Terminal) zusammenzufassen. Sie können dann direkt Benutzergruppen an den Terminals berechtigen (Siehe Kapitel 6.5), anstatt dies bei den einzelnen Benutzern machen zu müssen.

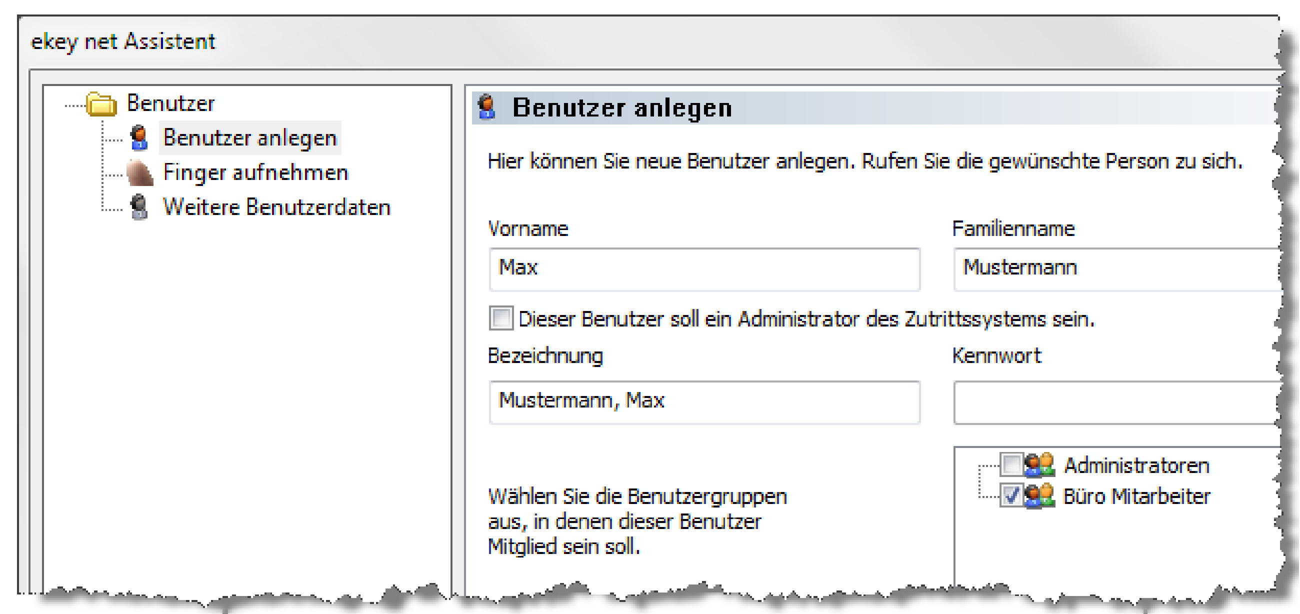
Im oben abgebildeten Beispiel wurden die Benutzernach Abteilungen zusammengefasst. Im ekey net Assistentendefinieren Sie wiederum den„**Namen**"der Benutzergruppe und Sie können auch hier eine **„Beschreibung"** hinzufügen.



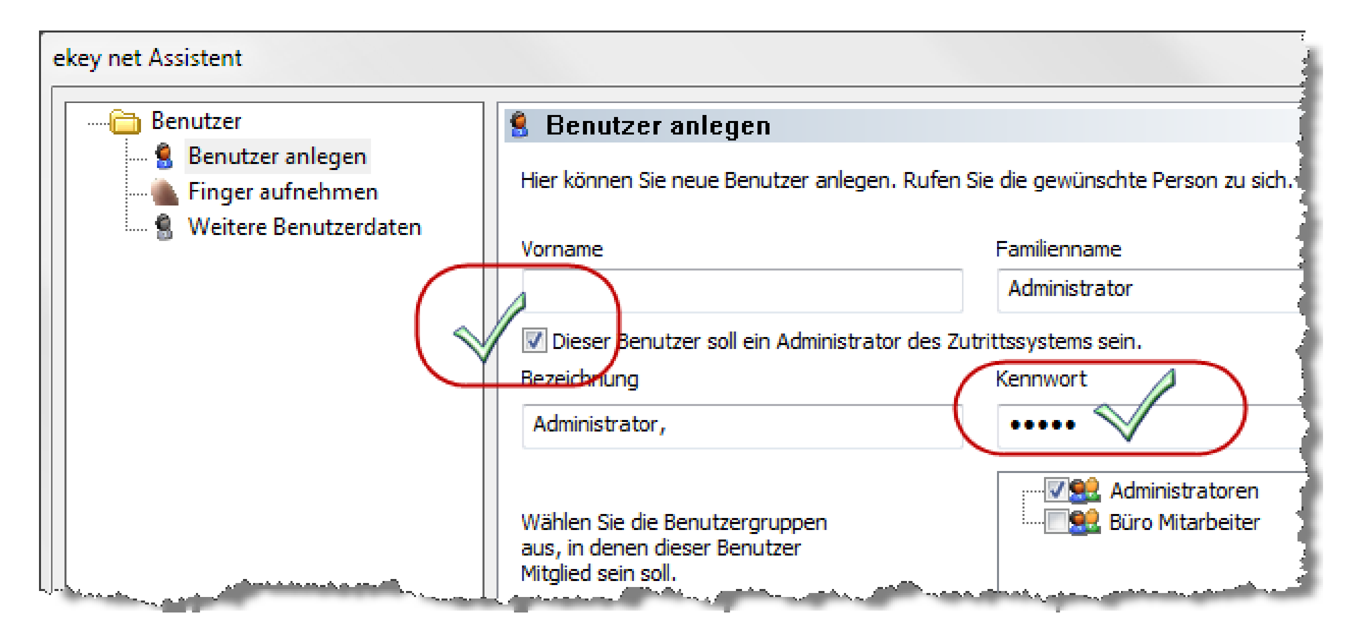
6.4.2.2 Benutzeranlage und Fingeraufnahme



Bei Klick auf den Menübutton „**Benutzer erstellen**" legen Sie einen neuen Benutzer an.Die Anlage des Benutzers erfolgt immer in der ausgewählten Firma und kann automatisch in dieBenutzergruppe verknüpft werden,welcheSie im ekey Assistenten per Mausklick gewählt haben.



Soll der **Benutzer auch als Administrator** des Zutrittssystems berechtigt werden, so müssen Sie diese Funktion aktivieren und durch die **Eingabe eines Kennwortes** vervollständigen!



<u>Das Feld Bezeichnung:</u>

Bezeichnung

Mustermann, Max

Der Inhalt des Bezeichnungsfeldes wird grundsätzlich automatisch aus den Feldern Vorname und Familienname erstellt. Bei der Anmeldung an der ekey net Software wird der Inhalt des Feldes Bezeichnung als



„Administrator"verifiziert – siehe Kapitel 6.1. Beachten Sie daher bei einer manuellen Änderung des Feldinhaltes folgende Hinweise:

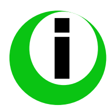


- *Der geänderte Inhalt des Feldes „Bezeichnung" muss 1:1 (Groß- und Kleinschreibung beachten) in das Feld „Administrator" des Anmeldedialoges übertragen werden – Vor- und Familienname sind in diesem Fall nicht von Bedeutung!*
- *Wird in weiterer Folge der Vor- und/oder der Familienname geändert, wird das Feld Bezeichnung automatisch aktualisiert und mit* ***„Familienname, Vorname"*** *befüllt*

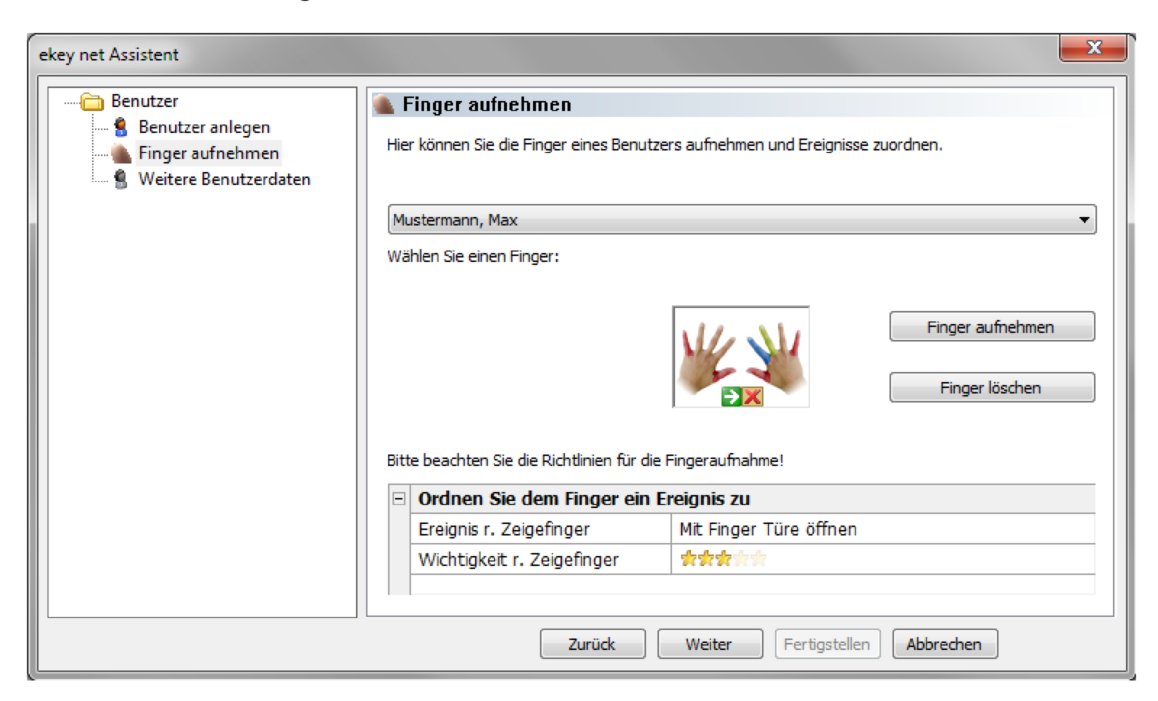
Deshalb wird von einer manuellen Änderung des Feldes „Bezeichnung" abgeraten!

Fingeraufnahme:

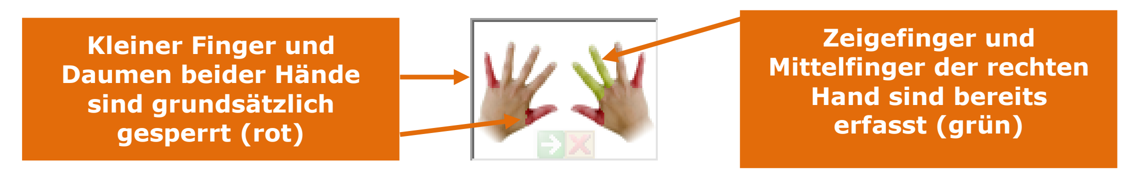
Im 2. Schritt des ekey Assistenten können Sie nun Finger aufnehmen und Ereignisse zuweisen (Details zu den Ereignissen finden Sie im Kapitel 8.1.3)



ekey net speichert keine Fingerbilder, sondern nur sogenannte Templates (binärer Code). Aus diesen Templates kann das ursprüngliche Fingerbild nicht zurückgerechnet werden.



Erklärung der Fingerfarben:

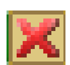




Die Sperre von Daumen und Kleiner Finger ist damit begründet, dass die Merkmale auf diesen Fingern sehr schlecht ausgeprägt sind und die Verwendung dieser Finger daher zu Fehlerkennungen führen könnte. Im Ausnahmefall kann diese Sperre über das Menü GRUNDEINSTELLUNGEN – OPTIONEN aufgehoben werden. Sicherheitstechnisch wird davon abgeraten!

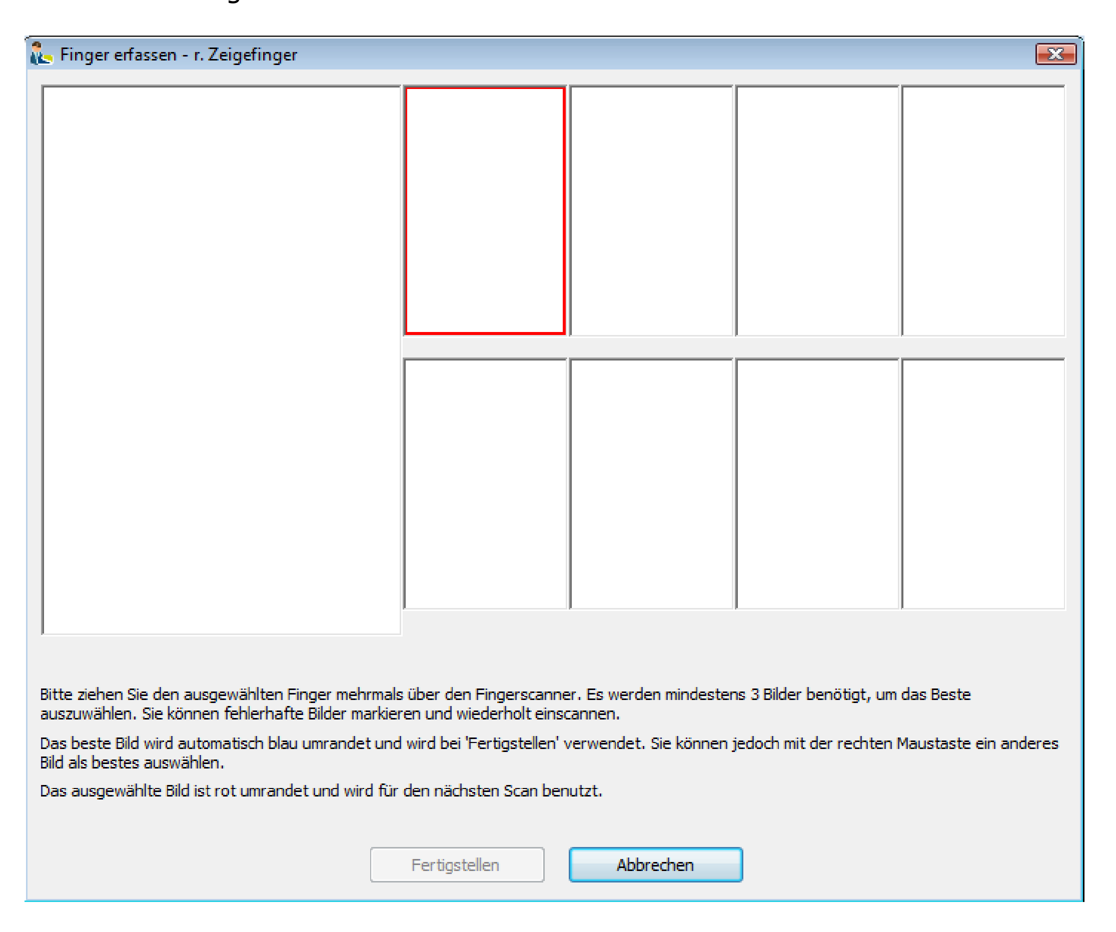
 Fingertemplate NEU

 Fingertemplate NEU (Überschreiben)

 Fingertemplate LÖSCHEN



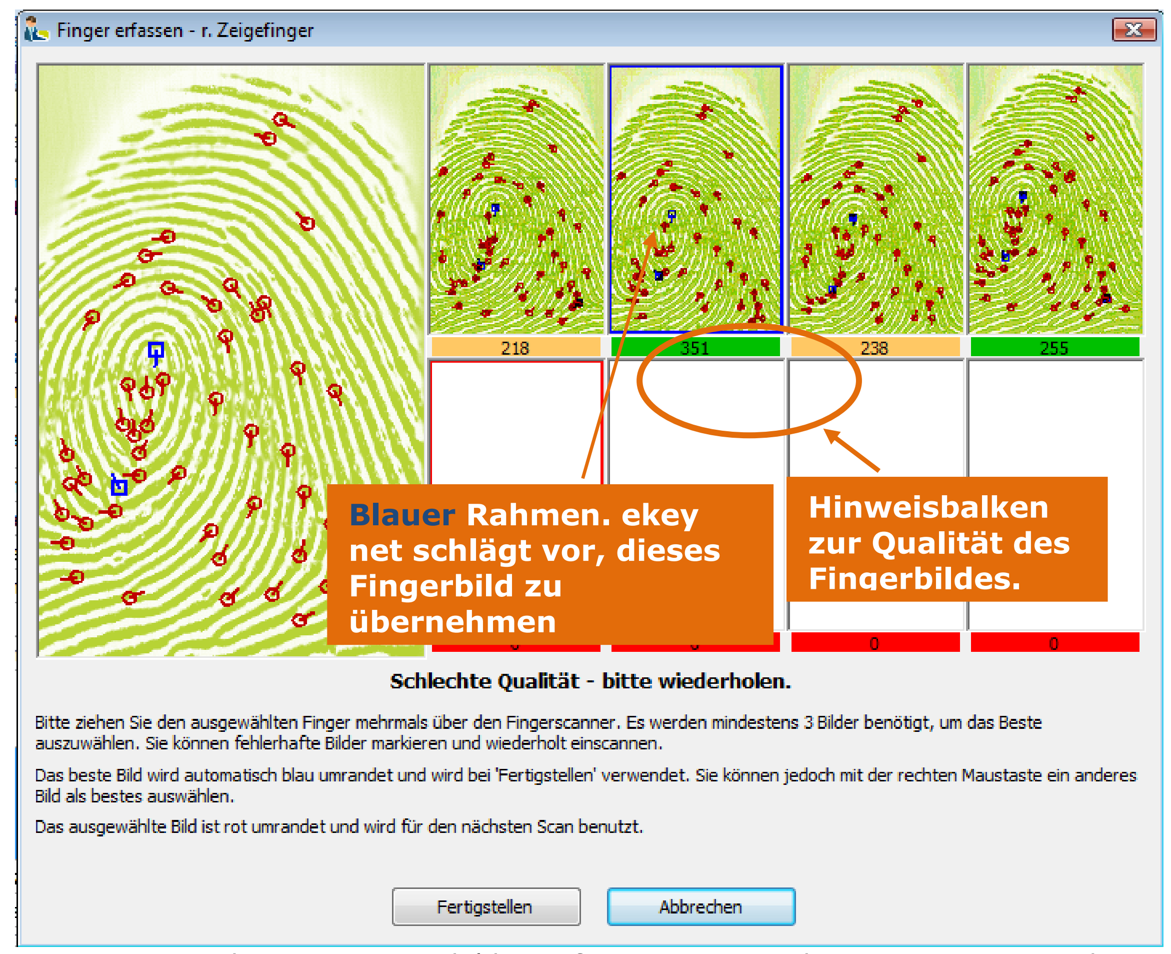
Zur Fingeraufnahme wählen Sie nun den Finger aus und klicken Sie dann auf das Symbol. 
Es erscheint folgendes Fenster:



Ziehen Sie nun den ausgewählten Finger gleichmäßig über das ekey bit (USB-Fingerscanner). Konzentrieren Sie sich dabei auf ein ordentliches Ziehen des Fingers und nicht auf die Finger-Bilder die im obigen Fenster erscheinen.



Je ordentlicher und konzentrierter Sie die Finger aufnehmen, je gewissenhafter Sie hier vorgehen, umso besser wird die Erkennungsleistung an denekey net FS sein. Beachten Sie bitte unbedingt auch zu diesem Thema den Film zur „Korrekten Fingerführung" auf der ekey net CD.
Nutzen Sie auch die Möglichkeit, den Finger mehrmals über den Sensor zu ziehen, um die richtige Fingerführung zu üben.



Es müssen mindestens 3 Fingerbilder aufgenommen werden. Die Bewertung der Fingerbilder sehen Sie dann direkt am Balken unter den Bildern:

… Fingerbild ist in Ordnung und für die Verwendung in ekey net OK
… Fingerbild ist noch gerade ausreichend für die Verwendung in ekey net. Sie können wenn Sie keine grünen Balken schaffen auch mit diesem Fingerbild arbeiten.
… Fingerbild ist sehr eingeschränkt brauchbar bis unbrauchbar.

Die Zahl im Balken ist ein weiterer Qualitätshinweis (= Score). Sie müssen aber nicht versuchen hier einen möglich hohen Wert zu erreichen, es reicht wenn der Balken **grün** ist.
Das System schlägt nun, nachdem Sie mehrere Bilder des gleichen Fingers aufgenommen haben, vor, welches Fingerbild (Template) ins System übernommen wird und an die Fingerscanner verteilt wird. Sie sehen diesen Vorschlag daran, dass das Fingerbild **blau** eingerahmt ist.
Wir empfehlen Ihnen diesen Vorschlag zu akzeptieren und mit Klick auf den Button Fertigstellen die Fingeraufnahme abzuschließen.



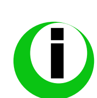
Es kann sein, dass Sie den Finger über das ekey Bit ziehen, aber kein Fingerbild erscheint. Dies ist normal. ekey net scheidet völlig unbrauchbare Bilder sofort aus und meldet nur **Schlechte Qualität - bitte wiederholen.** *Haben Sie Schwierigkeiten die Finger aufzunehmen, so sehen Sie sich bitte den Film „korrekte Fingerführung" auf der beiliegenden CD an.*

Ereigniszuordnung:
Als nächstes müssen Sie den erfassten Fingern auch ein entsprechendes Ereignis zuordnen, damit Sie Aktionen im System ausführen können. Diese Zuweisung erfolgt an dieser Stelle. Sie können jedem einzelnen Finger ein anderes Ereignis zuordnen, womit Sie die Möglichkeit haben mit 10 Fingern bis zu 10 verschiedene Ereignisse im System zu setzen.



Im Beispiel hier wurde dem „rechten Zeigefinger" das Ereignis „Mit Finger Türe öffnen" zugeordnet. Zur Funktion und Wirkung von Ereignissen siehe Kapitel 8.1.3

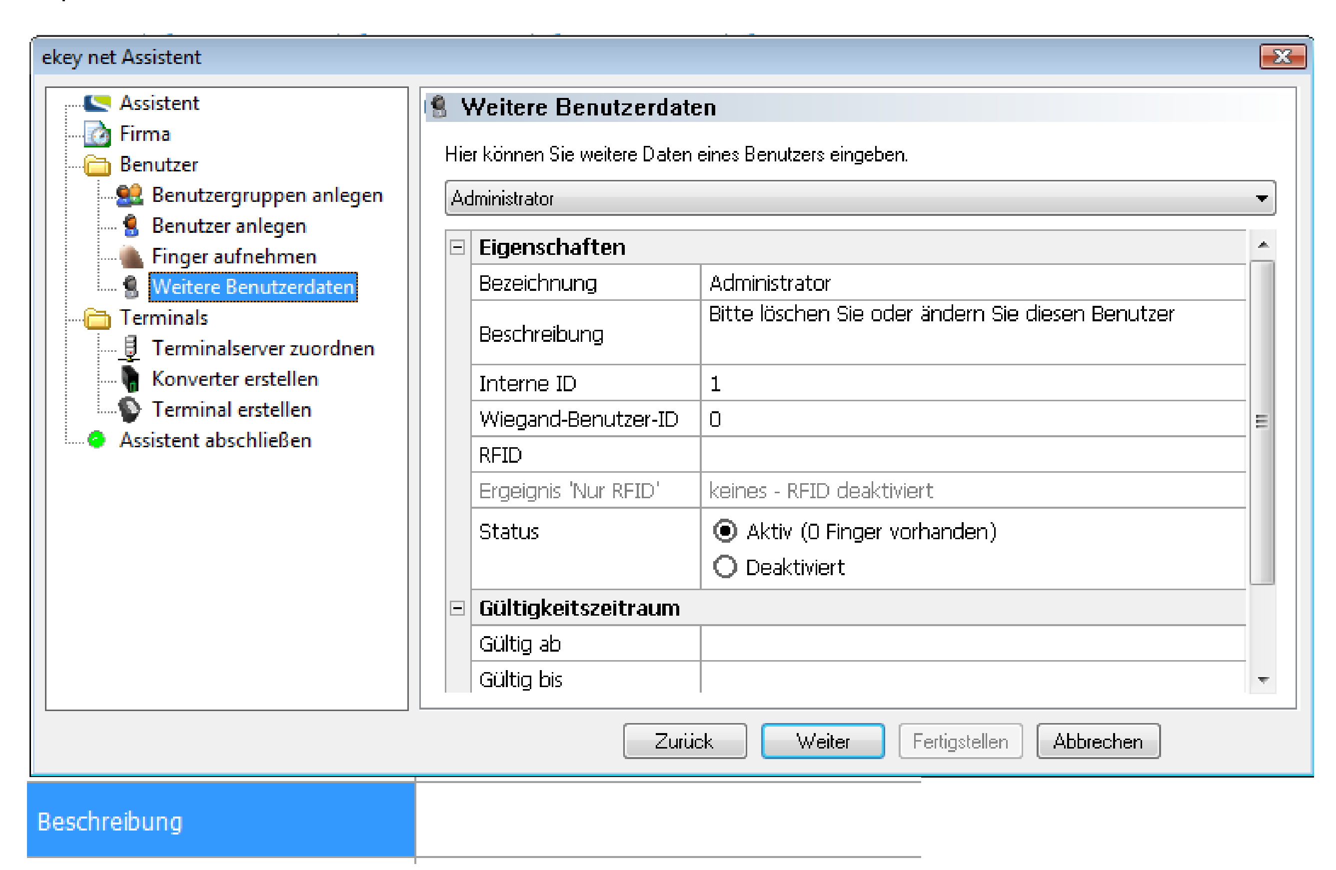
Eine spezielle Funktion liefert ihnen noch die „**Wichtigkeit**" des Fingers. Hier haben Sie die Möglichkeit bestimmten Benutzern (z.B. Geschäftsführung) eine schnellere Erkennung am Fingerscanner und damit eine schneller Freischaltung zu ermöglichen. Dies ergibt sich dadurch, dass Benutzer mit höherer Sterneanzahl vorrangig gereiht und die Referenz-Templates dieser Benutzer als erstes geprüft werden. Bei einer Neuanlage werden jedem Benutzer 3 Sterne zugeordnet. Sie können durch einen Mausklick die Wichtigkeit dann erhöhen oder vermindern.



Geben Sie allen Benutzern die gleiche Wichtigkeit, so führt auch ekey net eine intelligente Prüfung der Referenz-Templates durch. Abhängig davon, wie oft das System verwendet wird (Finger gezogen wird) wird die Reihenfolge der Prüfung der Referenz-Templates definiert. So haben Benutzer, die oft das System benutzen, schneller Zutritt.



Weitere Benutzerdaten:
Hier können Sie weitere Benutzerdaten eintragen. Auch jene Felder können befüllt werden, die Sie speziell imMenü „**OPTIONEN – Benutzerdaten**" konfiguriert haben. Siehe dazu auch Kapitel 8.1.6.

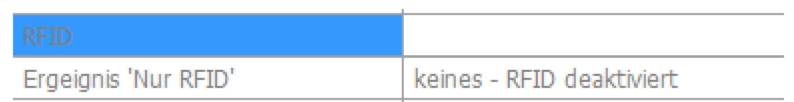


Beschreibung

Freie Eingabe von Daten für Hinweise zur Person bzw. besondere Funktionen, die die Person inne hat.



Hier tragen Sie die Wiegand – Benutzer ID ein. Sehen Sie dazu auch Kapitel 8.1.4.1.7



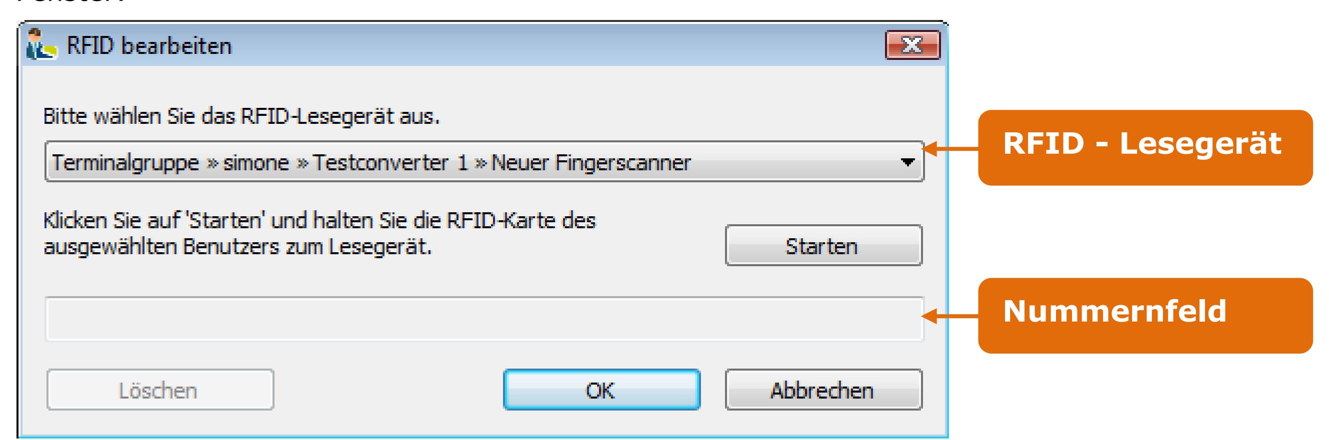
Möchten Sie einen Mitarbeiter berechtigen zusätzlich zu seinem Finger oder auch ausschließlich mit einer RFID-Karte zu arbeiten, so können Sie ihm hier die RFID-Kartennummer zuordnen.

ekey net arbeitet bei der RFID-Funktion ausschließlich mit der unverschlüsselten ID-Nummer der RFID - Karte. Diese Nummer kann nun hier erfasst und dem Benutzer zugeordnet werden.

Die Funktion muß unter den „Grundeinstellungen" im Menü „Optionen" aktiviert werden.



Machen Sie einen Doppelklick in das leere Feld RFID und es erscheint folgendes POPUP – Fenster:



Für die Nutzung der RFID- Funktion im ekey net müssen Sie diese vorher in den Optionen freischalten und konfigurieren. Sehen Sie dazu Kapitel 8.1.1



Um die RFID – Funktion zu nutzen müssen Sie auch die ekey net FS mit RFID Funktion ordern. Standardmäßig sind die ekey net FS nicht mit RFID ausgerüstet.

Wählen Sie nun das RFID-Lesegerät aus. In der Liste der Combo-Box sind alle Geräte gelistet, die im ekey net als RFID-Fingerscanner vorhanden und konfiguriert sind. Mit diesen Scannern können Sie die Kartennummer erfassen:

- ekey net FSRFID
- ekey net RFID-Leser USB

Nach Auswahl des RFID-Lesegerätes klicken Sie auf den Button Starten und halten Sie die RFID-Karte, die Sie dem Benutzer zuweisen möchten, vor das vorher ausgewählte Lesegerät. Die Kartennummer wird nun erfasst und in das Nummernfeld eingetragen. Der Lesevorgang ist damit beendet.
Mit klick auf den Button OK wird die Kartennummer dann aktiv dem User zugeordnet.

Klick auf Abbrechen führt zu einem Abbruch der RFID-Kartenerfassung.
Klick auf Löschen löscht die zugewiesene Kartennummer.



Nachdem Sie die RFID – Kartennummer erfasst haben, müssen Sie nun dieser Karte auch ein Ereignis zuordnen, welches ausgeführt wird, sobald die Karte bei einem berechtigten ekey net FS vorgehalten wird. Grundsätzlich sind hier alle im System bekannten Ereignisse zuordbar. Siehe dazu auch Kapitel 8.1.3.



Haben Sie bei einem Fingerscanner die RFID-Verwendung RFID + Finger verwenden *gewählt, so ist die Zuweisung dieses Ereignisses wirkungslos. Es wird immer das dem,in Kombination verwendeten, Finger zugewiesene Ereignis ausgeführt!*

Status	◉ Aktiv (1 Finger vorhanden) ○ Deaktiviert

Im Status sehen Sie, ob der Benutzer im System aktiviert oder deaktiviert ist. Nur ein aktivierter Benutzer kann im System Ereignisse auslösen.
Der Benutzer ist automatisch deaktiviert:

- wenn keine Finger **oder**
- keine RFID-Kartenummer

erfasst sind.
ekey net aktiviert automatisch Benutzer, wenn ein Finger eingelesen, oder eine RFID-Karte zugewiesen wird. Administratoren können Benutzer per Mausklick deaktivieren.

Gültigkeitszeitraum	
Gültig ab	
Gültig bis	

zeigt Ihnen an, ab wann oder bis wann dieser Benutzer im System gültig ist, und damit Ereignisse auslösen kann. Diese Funktion kann beispielsweise für Personen verwendet werden, die sich nur begrenzte Zeit im Unternehmen bewegen, wie z.B. Ferial-Praktikanten. Ist der Gültigkeitszeitraum abgelaufen, so wird der Benutzer automatisch deaktiviert und verbleibt ohne Berechtigungen im System.

Weitere Benutzerdaten

Hier können Sie weitere Benutzerdaten eintragen. Auch jene Felder können befüllt werden, die Sie speziell im Menü „**OPTIONEN – Benutzerdaten**" konfiguriert haben. Siehe dazu auch Kapitel 8.1.6.

Folgende Daten werden vom System vergeben, und können von Ihnen nicht geändert werden:

- Interne Benutzer ID
  Wird vom System automatisch erstellt. Diese ID ist beim Datenlogging von spezieller Bedeutung. Sehen Sie dazu auch Kapitel 15
- Bezeichnung (wird aus Vor und Nachname automatisch erstellt)

6.4.3 Bearbeiten von Benutzern und Benutzergruppen

6.4.3.1 Änderung von Parametern

Benutzergruppen und Benutzer können jederzeit bearbeitet und die entsprechenden Parameter überschrieben werden. Markieren Sie das gewünschte Objekt und starten Sie den ekey net Assistenten.



Änderungen der Objekte werden grundsätzlich immer mit dem Assistenten durchgeführt. Mit der Funktion **Objekt öffnen** wird dieser passend zum entsprechenden Objekt gestartet.

Objekt öffnen



6.4.3.2 Force Update

Bei „Änderungen an Terminals senden“, werden nur die Änderungen an die Geräte übermittelt. Drücken Sie gleichzeitig mit dem Klickauf den Button auch die Tasten „STRG“ und „SHIFT“, so wird ein sogenanntes „**FORCE UPDATE**“ durchgeführt, welches alle Informationen nochmals gesammelt zu den Fingerscannern übermittelt.

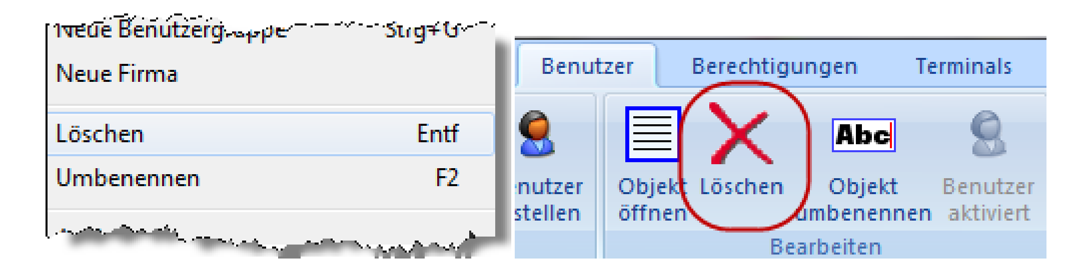
Besonders sollten Sie dies durchführen:

- wenn ein Benutzer gelöscht wurde (darf keinen Zutritt mehr haben)
- wenn Sie mehrere Änderungen gleichzeitig gemacht haben.
- bei der Neukonfiguration

Dadurch werden Änderungen im System aktiv !

6.4.4 Löschen von Benutzern und Benutzergruppen

KlickenSie mit der rechten Maustaste einfach auf den zu löschenden Benutzer bzw. die Benutzergruppe. Es erscheint das Kontext-Menü:



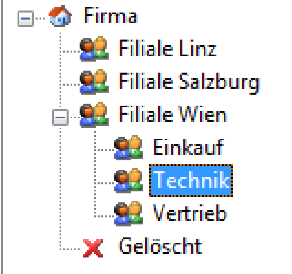
Wählen Sie hier „**Löschen**“ oder Klicken Sie in der Symbolleiste **„Bearbeiten“ auf Löschen**



Beim Löschen von Benutzergruppen werden auch alle Benutzeruntergruppen mit gelöscht. Die Benutzer bleiben aber in der übergeordneten Firma erhalten! Benutzer müssen immer definitiv einzeln gelöscht werden und können NICHT durch Löschen der Benutzergruppe gelöscht werden!

Abschließend führen Sie ein „**Force Update**“ lt. Kapitel 6.4.3.2 durch.
Dadurch wird die Änderung im System aktiv !

Wichtig ist hier noch anzumerken, dass die Benutzer nicht sofort unwiederbringlich aus dem System gelöscht, sondern im Benutzerexplorer unter dem Bereich Gelöscht abgelegt werden. Sie können somit ein irrtümliches Löschen rückgängig machen, indem Sie die Benutzergruppe einfach wieder in die „aktive“ Benutzergruppe“ mit Drag&Drop verschieben. Erst wenn Sie den Inhalt von Gelöscht leeren, sind die Daten unwiederbringlich verloren.



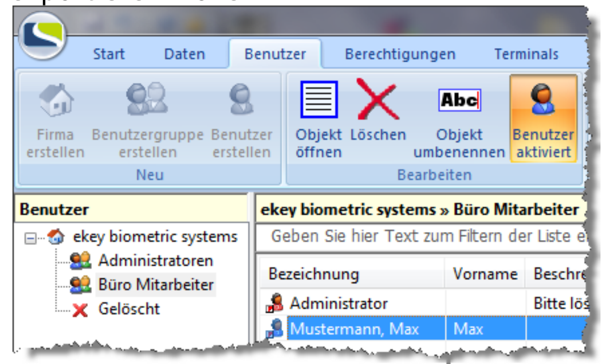


6.4.5 Benutzerexport und -import

Sie können die Daten von Benutzern und Benutzergruppen inklusiv deren Finger-Templates aus ekey net exportieren und in ein anderes System wieder importieren. Dies ist z.B. bei einer Übersiedlung ihrer Firma / Organisation sehr vorteilhaft, da Sie die Finger der Mitarbeiter nicht neu aufnehmen müssen.

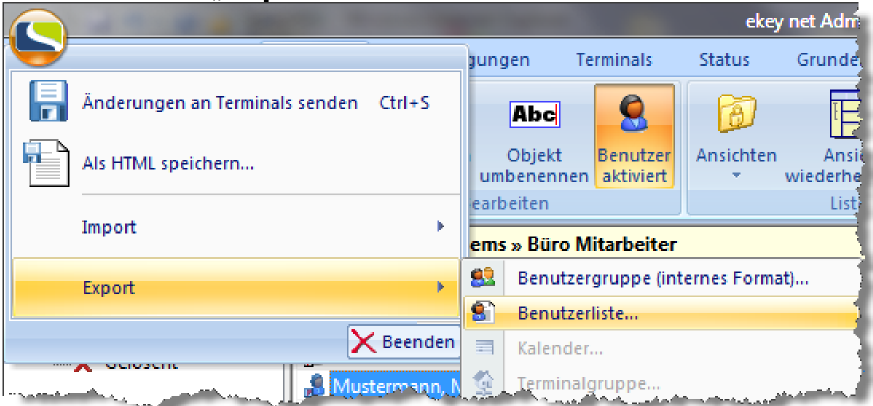
6.4.5.1 Benutzerexport

Für einen Export wählen Sie im Benutzer-Explorer die Benutzerbzw. Benutzergruppe die Sie exportieren wollen.



Hier z.B. wird der Benutzer „Max Mustermann" aus der Benutzergruppe „Büro Mitarbeiter" exportiert

Klicken Sie dann mit der linken Maustaste auf das ekey Symbol links oberhalb der Menüleiste und wählen Sie „**Export**"



Bei **Benutzergruppe(internes Format)**wird

- eine interne Datei kreiert,
- dieSie an einem wählbaren Speicherort
- mit definierbarem Dateinamen

ablegen können.

Dieses File beinhaltet alle Benutzerdaten inklusive der Finger-Templates aber ohne Berechtigungsstruktur,welches Sie dann jederzeit in eine andere oder in dieselbe ekey net Installation wieder importieren können.

Bei **Benutzerliste** wird ein Export der Benutzerdaten **OHNE**Finger-Templates exportiert. Mögliche Exportformate:

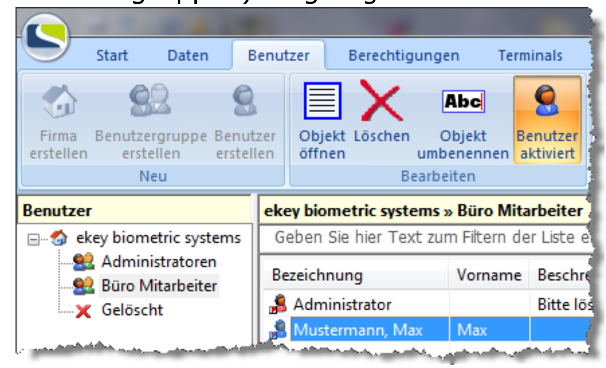
- .XML
- .XLS
- .CSV

Beispiel eines XML Exports:

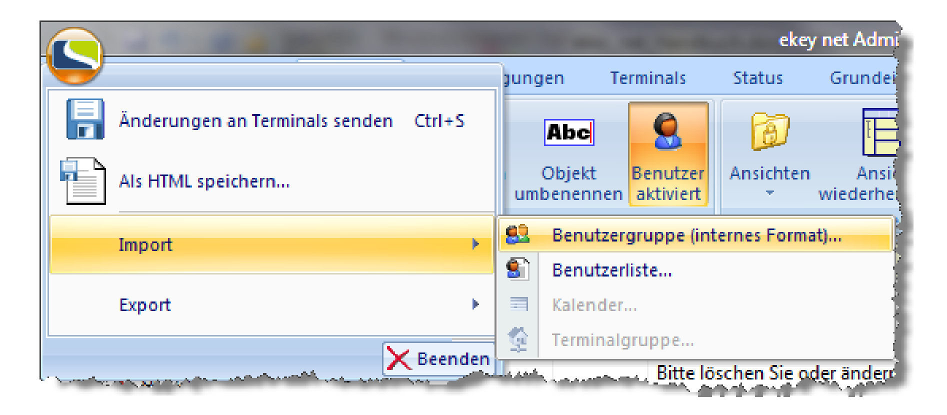
```
<?xml version="1.0" ?>
- <USERS>
  - <Benutzer>
      <Bezeichnung>Mustermann, Max</Bezeichnung>
      <Vorname>Max</Vorname>
      <Nachname>Mustermann</Nachname>
      <Beschreibung />
      <Status>Aktiv</Status>
      <Anmeldename />
      <Login>mustma</Login>
    </Benutzer>
  </USERS>
```

6.4.5.2 Benutzerimport

Wählen Sie die Terminalgruppe, in welchedie zu importierenden Benutzer (bzw. Benutzergruppen) eingefügt werden sollen.



Anschließend klickenSie mit der linken Maustaste auf das ekey Symbol.



Wählen Sie nun „**Import**" und wieder eines der Formate:

Benutzergruppe: Benutzer (bzw. Benutzergruppen) mit Finger-Templates
Benutzerliste: nur Daten ohne Finger-Templates

Es öffnet sich der Windows – Dialog zur Auswahl des entsprechenden Files und nach Ihrer Wahl werden die Daten im gewünschten Bereich der Benutzerstruktur eingefügt.



6.5 Menü „BERECHTIGUNGEN“

In der Berechtigungsebene erfolgt nun die Zuordnung Wer- Wann- Wo Aktionen auslösen kann.

Bevor Sie mit der eigentlichen Vergabe der Berechtigungen beginnen, müssen Sie die **Zeitfenster (Kapitel 6.6.6)**und **Kalender (Kapitel 6.6.7)**in den einzelnen Terminalgruppen definieren

6.5.1 Berechtigungen

Hier definierenSie, wann, wer, wo Zutritt hat bzw. ein Ereignis mit seinem Finger auslösen kann. Die Berechtigungen werden **benutzerbezogen** vergeben. Das heißt, dass ein Zeitfenster an einem Terminal immer für alle Finger eines Benutzers gilt.

Die Darstellung der berechtigungsebene:

Terminals
Terminalgruppen
Filiale Linz
Filiale Salzburg
Filiale Wien
Zutrittsberechtigung erstellen oder löschen: Doppelklick oder Drag&Drop
Bürozeit
Immer
Filiale Linz
Filiale Salzburg
Filiale Wien
Brunner, Manfred
Kräftner, Heinz
TOCAadmin
Benutzer
Firma
Filiale Linz
Filiale Salzburg
Filiale Wien
Terminal-gruppen
Zeitfenster der gewählten Terminalgruppe
Benutzer der gewählten Benutzer-gruppe
Benutzer-gruppen
Berechtigungs-fenster

6.5.1.1 Vergabe der Berechtigungen

Um eine Berechtigung zu vergeben gehen Sie nun wie folgt vor:

Terminalwahl:
Wählen Sie mit einem Mausklick die Terminalgruppe / das Terminal (Fingerscanner) auf dem Sie eine Benutzergruppe bzw. einen Benutzer berechtigen möchten:

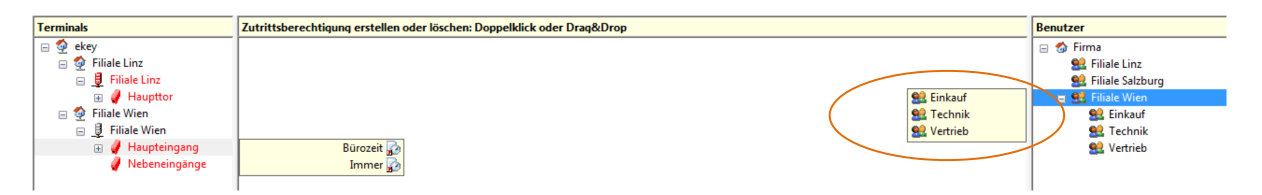


Die Zeitfenster der Terminalebene sehen Sie nun im Berechtigungsfenster



Benutzerwahl

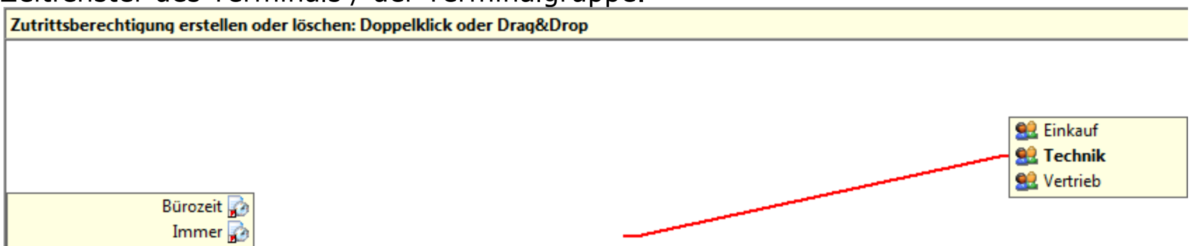
Wählen Sie nun mit einem Mausklick den /die gewünschte(n) Benutzer / Benutzergruppe die Sie am gewählten Terminal (Terminalgruppe) berechtigen möchten.



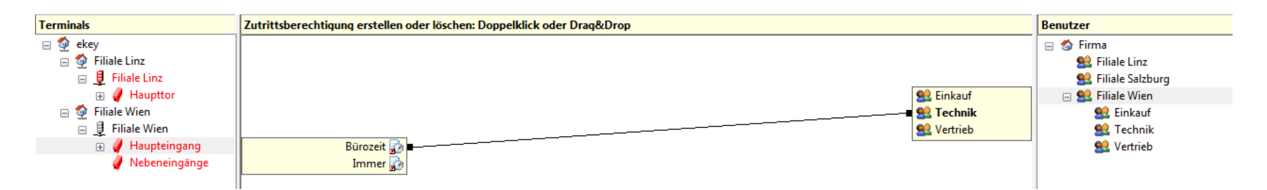
Im Berechtigungsfenster erscheinen die Untergruppen bzw. die Benutzer der gewählten Benutzergruppe.

Berechtigungsvergabe

Klicken Sie dafür auf den / die Benutzer / Benutzergruppe im Berechtigungsfenster mit der linken Maustaste und halten Sie diese gedrückt. Ziehen Sie diese dann zum gewünschten Zeitfenster des Terminals / der Terminalgruppe.



In diesem Fall wird die Benutzergruppe „Technik" der Filiale Wien mit dem Zeitfenster „Bürozeit" der Terminalgruppe „Haupteingang" verbunden.



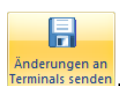
Die Farbe der Verbindungslinie können Sie in den Eigenschaften des Zeitfensters definieren (Siehe dazu auch Kapitel 6.6.6).

Das Beispiel hier zeigt, dass alle Benutzer der Benutzergruppe „**Technik**" der Filiale Wien in der „**Bürozeit**" an den Terminals, die dem ekey net CV LAN „**Haupteingang**" zugeordnet sind, Zutritt haben.

STOP

Achten Sie bei der Vergabe der Berechtigungen, dass Sie Benutzer pro Terminal keine überlappenden Zeitfenster zuweisen! Dies kann zu Fehlfunktionen führen!
Als Beispiel: Hr. Mustermann bekommt am Fingerscanner Haupteingang die Berechtigung: Immer = 0-24Uhr von Mo-So
und Selbsthaltung Geschäft: = Selbsthaltung 8:00 Uhr -18:00Uhr
ekey net weiß nun nicht, was gilt -> normales Öffnen oder Selbsthaltung -> Es kann somit sein, dass die Selbsthaltung nicht funktioniert.
Definieren Sie vor diesem Hintergrund die Zeitfenster entsprechend und weisen Sie keine überlappenden Zeitfenster zu!!!

Änderungen an Terminals senden


Klicken Sie nach Abschluss der Konfiguration und Berechtigungsvergabe auf .

Erst jetzt werden die Einstellungen an die Terminals gesandt und damit aktiviert!

Sie müssen dies nicht nach jeder Änderung machen, sondern können dies am Ende der Durchführung alle Einstellungen, vor dem Verlassen des ekey net Admin durchführen.

6.5.1.2 Force Update

Bei „Änderungen an Terminals senden" Änderungen an Terminals senden, werden nur die Änderungen an die Geräte übermittelt. Drücken Sie gleichzeitig mit dem Klickauf den Button auch die Tasten „STRG" und „SHIFT", so wird ein sogenanntes „**FORCE UPDATE**" durchgeführt, welches alle Informationen nochmals gesammelt zu den Fingerscannern übermittelt.

Besonders sollten Sie dies durchführen:

- wenn ein Benutzer gelöscht wurde (darf keinen Zutritt mehr haben)
- wenn Sie mehrere Änderungen gleichzeitig gemacht haben.
- bei der Neukonfiguration

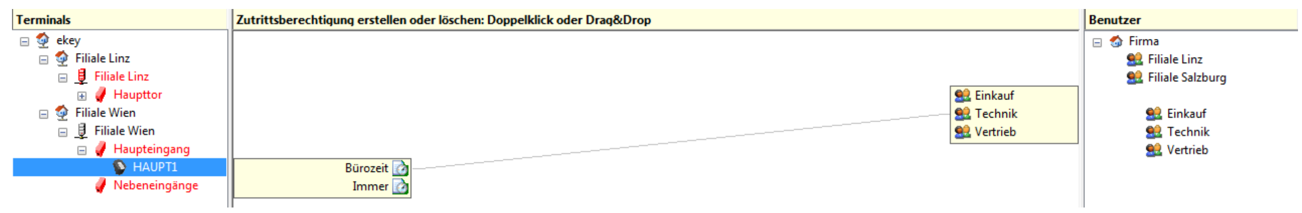


Prüfen Sie immer die Berechtigungsänderungen durch Stichproben direkt an den Fingerscannern. Nur so können Sie sicherstellen, dass die getätigten Änderungen auch ihrem Wusch entsprechen !

6.5.1.3 Vererbung

Berechtigungen werden in Abhängigkeit der Einstellungen in den Optionen (siehe Kapitel 8.1.1 an hierarchisch darunter liegende Ebenen in den Terminalgruppen vererbt. Vererbte Berechtigungen werden im Berechtigungsfenster

- grau dargestellt und
- können auf der vererbten Ebene nicht gelöscht werden.



In unserem Beispiel wurde die Berechtigung für die Benutzergruppe „**Technik**" auf der Terminalgruppe „Haupteingang" vergeben. Sieht man nun die Berechtigungen des Terminals „**HAUPT1**" an, so sieht man, dass die Gruppe „**Technik**" mit dem Zeitfenster „Bürozeit" berechtigt ist.Die Berechtigungslinie (Verbindungslinie) ist aber grau und kann nicht gelöscht werden. Die Berechtigung ist also geerbt.

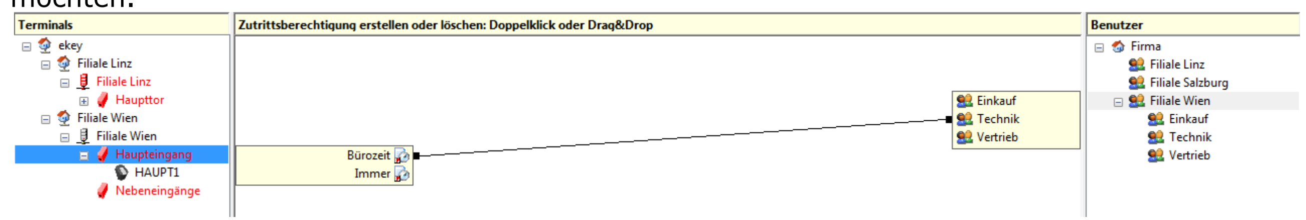
6.5.1.4 Berechtigungen Löschen oder ändern

Berechtigungen können jederzeit gelöscht werden. Die Löschung kann nur in den Terminalebenen / Benutzerebenen erfolgen, wo Sie auch erstellt wurden. Geerbte Berechtigungen sind nicht löschbar.

Löschen Sie die Berechtigung wie folgt:

Wahl Terminalgruppe und Benutzergruppe

Wählen Sie die Terminalgruppe und die Benutzergruppe, der Sie die Berechtigung entziehen möchten.



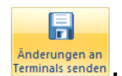
Löschen oder Ändern der Verbindungslinie

Klicken Sie entweder auf der Benutzerseite oder der Zeitfensterseite auf das Rechteck.



- Bei einem Klick wird die Linie und damit die Berechtigung gelöscht
- Durch Klick und Halten der Maustaste, kann die Linie neu zugeordnet werden

Änderungen an Terminals senden

Klicken Sie nach Abschluss der Änderung auf 
.

Erst jetzt werden die Änderungen an die Terminals gesandt und damit aktiviert.

Sie müssen dies nicht nach jeder Änderung machen, sondern können dies am Ende der Durchführung aller Einstellungen, vor dem Verlassen des ekey net Admin durchführen.


Das Löschen bzw. Ändern vererbt sich natürlich auch in Abhängigkeit der Einstellungen bei den Optionen auf die hierarchisch darunterliegenden Terminalgruppen.



6.6 Menü „TERMINALS“

6.6.1 Allgemeines zur Konfiguration

Die Terminalebene erlaubt die Konfiguration von ekey net auf Geräteseite (physikalische Ebene).

- Hier wird das System mit den einzelnen Geräten in Betrieb genommen.
- Hier werden die Aktoreinheiten (ekey net SE) den Sensoreinheiten (ekey net FS) zugeordnet.
- Die Systemarchitektur ihrer Anlage wird hier definiert.

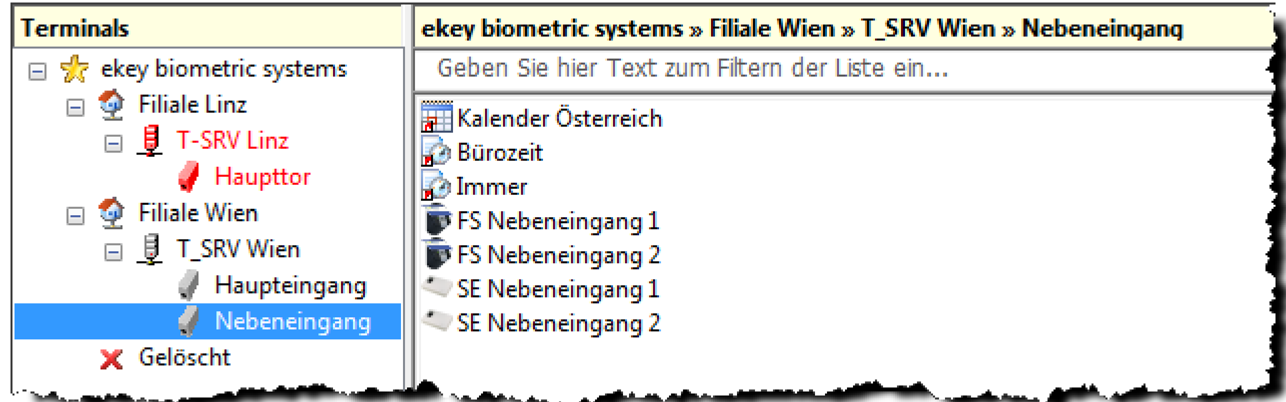
Bevor Sie mit der Konfiguration beginnen, klären Sie, wie sich die Architektur ihres Systems darstellt. Sie müssen hier wissen, wie ihr System verkabelt ist bzw. wie Sie es betreiben möchten um alle ihre Anforderungen zu erfüllen. Hier ein Beispiel eines verkabelten Systems:

ekey net Masterserver
Masterserver „ekey“
ekey net Terminalserver
Filiale Wien
ekey net Terminalserver
Filiale Linz
Ethernet 10Base T / 100Base- TX
Nebeneingänge
Haupteingang
Haupttor
ekey converter LAN
ekey converter LAN
ekey converter LAN
RS485
FS NEBEN1
ekey net S Fingerscanner
FS HAUPT
ekey net L RFID-Fingerscanner
FS TOR
ekey net S Fingerscanner
SENEBEN1
ekey net M Steuereinheit
SE HAUPT
ekey net M Steuereinheit
SETOR
ekey net M Steuereinheit
FS NEBEN 2
ekey net M Fingerscanner
SENEBEN2
ekey net M Steuereinheit

Im obigen Beispiel sind unter einem ekey net Masterserver zwei ekey net Terminalserver für die Filialen in Linz und Wien platziert. In Linz gibt es nur einen ekey net CV LAN, der einen ekey net FS und eine ekey net SE verwaltet.

In Wien gibt es 2 ekey net CV LAN, wobei einer die Geräte der Nebeneingänge und einer die Geräte für den Haupteingang verwalten. Die Verdrahtung des RS485 Busses und das Ethernet ist analog wie oben gezeichnet.

Im ekey net stellt sich dies dann in der Terminalstruktur für die Nebeneingänge in Wien so dar:



Machen Sie ebenfalls für Ihr System diesen Plan und beginnen Sie erst dannmit der Parametrierung ihres Systems. Es wird dann wesentlich einfacher und übersichtlicher.



*In dieser Ebene ist **NICHT** bekannt:*

- *Welche Benutzer welche Ereignisse auf dem Fingerscanner auslösen.*
- *ob eine zeitliche / kalendarische Berechtigung zur Ereignisauslösung vorliegt.*

Deshalb erfolgt noch keine Aktionsausführung im System ohne die entsprechenden Konfigurationen von BENUTZER- und BERECHTIGUNGSEBENE.



Bevor Sie hier mit der Konfiguration beginnen, prüfen Sieob alles ordnungsgemäß verkabelt und mit Spannung versorgt ist. Beachten Sie dabei die Empfehlungen lt. Verkabelungsplänen und der „ekey net Spezifikation".

6.6.2 Ablauf der Konfiguration auf Terminalebene

Klicken Sie den Menübereich „**Terminals**", so erscheint folgende Symbolleiste, welche Ihnen nun die Konfiguration der Terminals erlaubt.

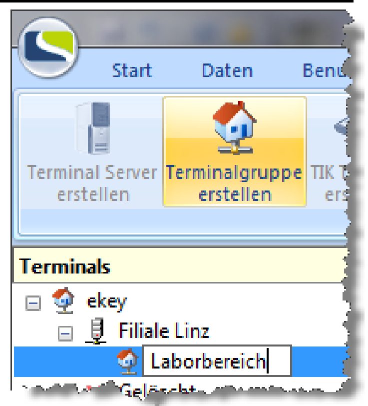


Um die Wahrscheinlichkeit von Fehlern so gering als möglich zu halten, können je nach „Zielort" für das neue Objekt nur für diesen Bereich gültige Objekte erstellt werden:

1 **Aktives Objekt** – dieses kann erstellt werden

2 **Inaktives Objekt** – dieses kann in der gewünschten Zielebene nicht erstellt werden oder ist nicht aktiv! zB.: Wenn kein ekey net CV LANkonfiguriert ist, können auchkeine Fingerscanner erstellt werden!

6.6.3 Parametrierung der Terminalgruppen und Geräte



Generell istfür die Inbetriebnahme des Systems und die Parametrierung der Geräte der „ekey net Assistent" (siehe Kapitel 7) zu verwenden.

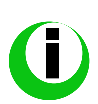
Insbesondere aber können Sie Terminalgruppen „manuell" erstellen und mit einer Bezeichnung versehen.

6.6.3.1 Terminalgruppen

Im ekey net können Sie, um

- eine bessere Systemübersicht über ihre Geräte und
- eine einfachere und übersichtliche Berechtigungsstruktur

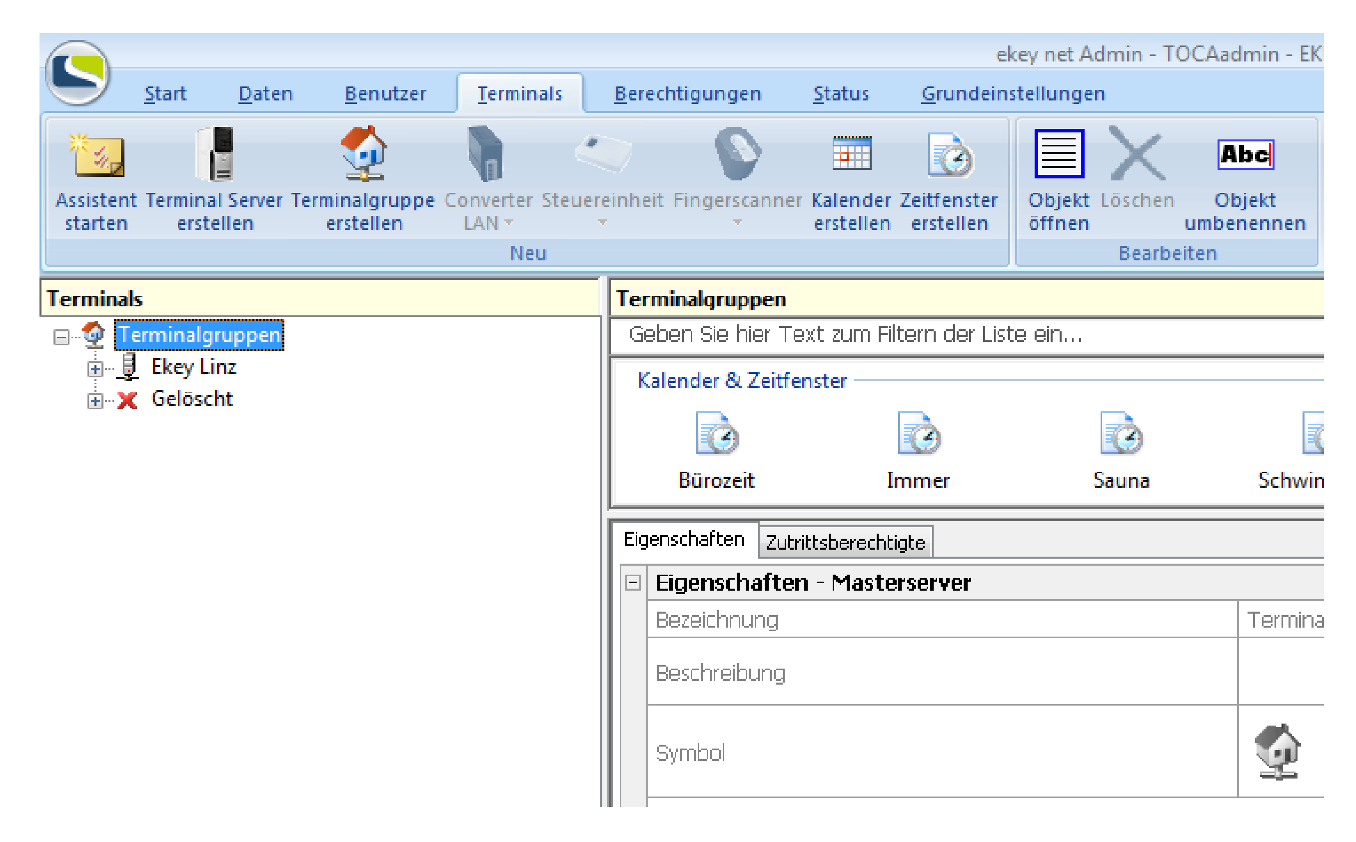
zu haben, Terminalgruppen anlegen. Die Anlage erfolgt im Menüreiter „Terminals"



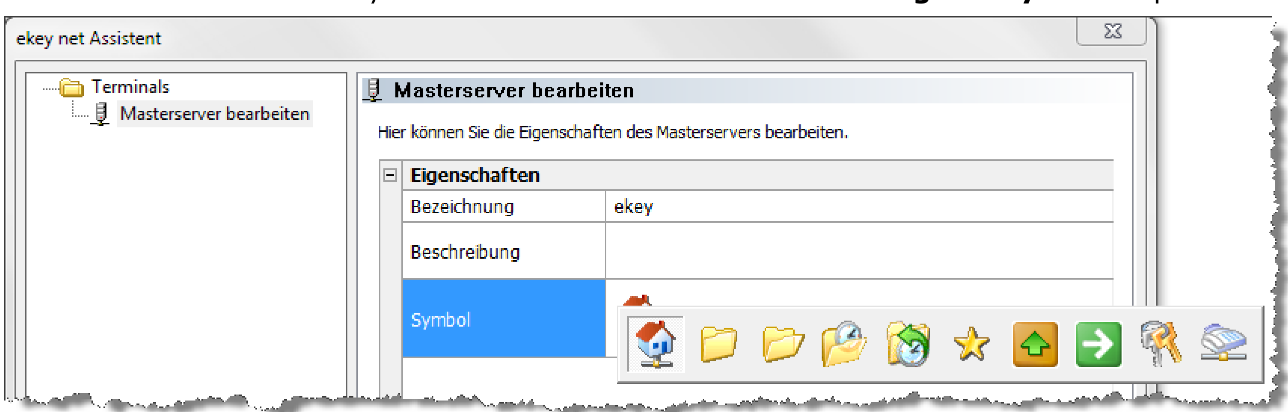
Bilden Sie in den Terminalgruppen die Systemarchitektur ab und berücksichtigen Sie dabei auch die Zutritts-Rechte von Benutzergruppen. Fassen Sie Geräte / ekey net CV LAN / ekey net Terminalserver, auf denen Sie idente Benutzergruppen berechtigen, zu Gruppen zusammen. Das System wird dann wesentlich übersichtlicher und die Wartung viel einfacher.

Die **„Stammebene"** -> sozusagen die Darstellung des ekey net Masterservers ->ist bereits vorgegeben und kann mit einem Mausklick ausgewählt werden. Durch einen weiteren Klick auf das Symbol **„Objekt öffnen"** Objekt öffnen





können Sie wieder den ekey net Assistent starten und **Bezeichnung** und **Symbol** anpassen:



Durch Klick auf den Menü-Button „**Terminalgruppe erstellen**" können Sie weitere Ebenen festlegen. So können Sie z.B. Filialbetriebe klar erkennen. Gleichzeitig kann aber eine Terminalgruppe auch durch folgende Objekte

- ekey net Terminalserver
- ekey net CV LAN

definiert sein. Die Erstellung können Sie durch Klick auf das jeweilige Symbol machen.



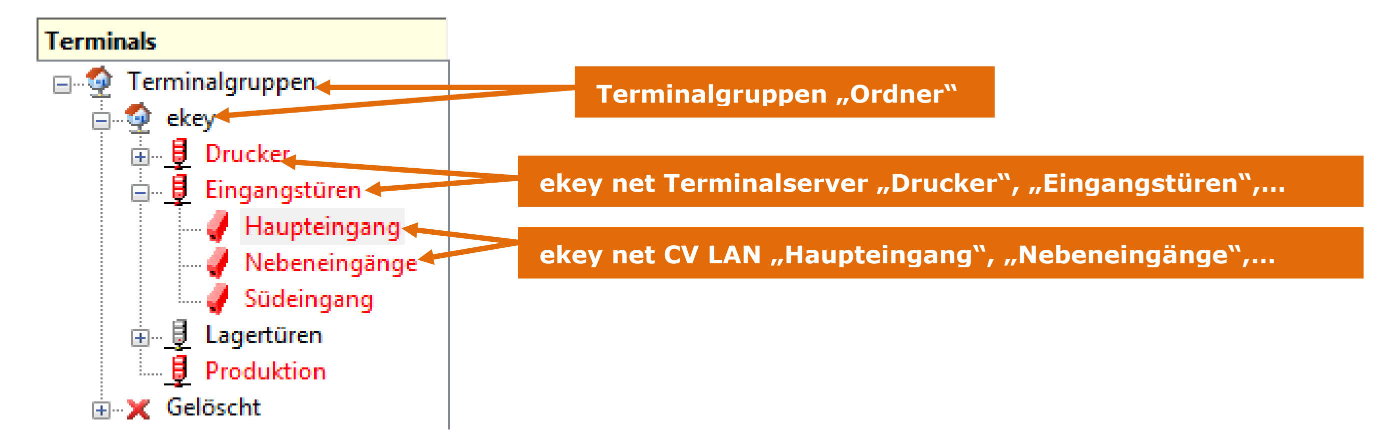
Es gibt also 3 Arten (Typen) von Terminalgruppen:

- Die Art „**Verwaltung**" (Terminalgruppe), = Ordnerfunktion wie im MS-Explorer zur Organisation der Gruppen
- **ekey net Terminalserver**
- **ekey net CV LAN**

Der Aufbau ist hierarchisch so zu sehen, dass es übergeordnet Terminalgruppen der Art „**Verwaltung**" gibt. In diesen Terminalgruppen kann es dann einen oder mehrere (grundsätzlich unbegrenzte Anzahl) ekey net Terminalserver geben(ausgenommen LIGHT).

Unter einem ekey net Terminalserver können dann einer oder mehrere (grundsätzlich unbegrenzte Anzahl) ekey net CV LANplatziert sein. Um mehrere ekey net CV LAN in einer „Verwaltungsgruppe" zusammen zu fassen, kann man natürlich dazwischen wiederum eine „Ordner" – Terminalgruppe einfügen.

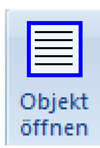
Und zuletzt können unter einem ekey net CV LAN maximal 8 Geräte verwaltet werden (z.B. 5ekey net FS + 3 ekey net SE).

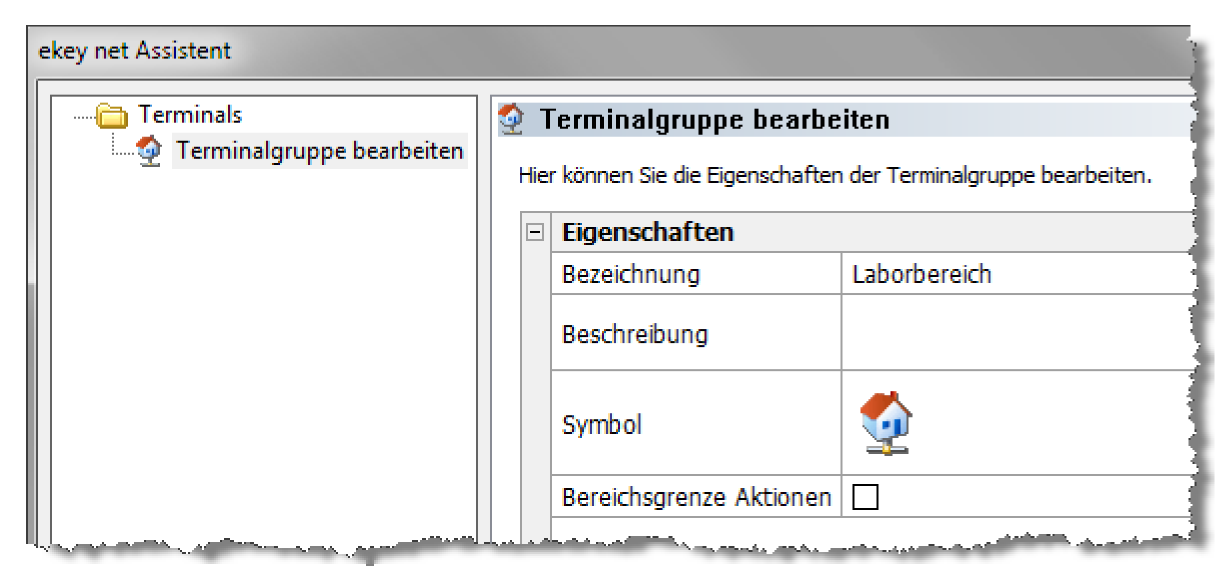


Die Eigenschaften der Terminalgruppen können im ekey net Assistent zugeordnet werden. Die dabei einzustellenden Werte sind natürlich abhängig von der Art der Terminalgruppe.

6.6.3.1.1 Konfigurationeiner Terminalgruppe „Verwaltung“

Nach Erstellung der Terminalebe markieren Sie diese und starten den ekey net Assistent durch Klick auf die Schaltfläche **„Objekt öffnen“**





Unter „**Eigenschaften**“ können Sie folgende Details eintragen oder ändern.

Bezeichnung:

Bezeichnung	Filiale Linz

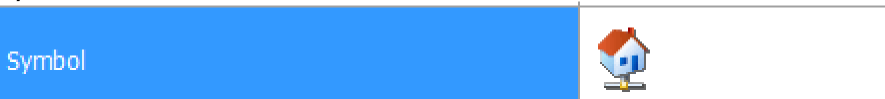
Hier definieren Sie die Bezeichnung der Terminalgruppe. Diese Bezeichnung wird auch im Terminalexplorer angezeigt.

Beschreibung:

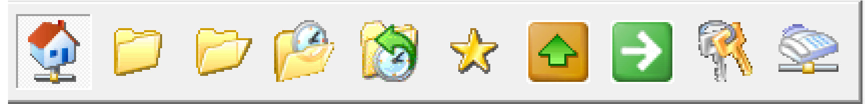
Beschreibung	

Freies Beschreibungsfeld für Informationen zu der Terminalgruppe

Symbol



Hier können Sie der Terminalgruppe ein Symbol zuordnen. Folgende Symbole stehen zur Auswahl



Das Symbol wird dann im Terminalexplorer der Bezeichnung vorangestellt.

z.B. 



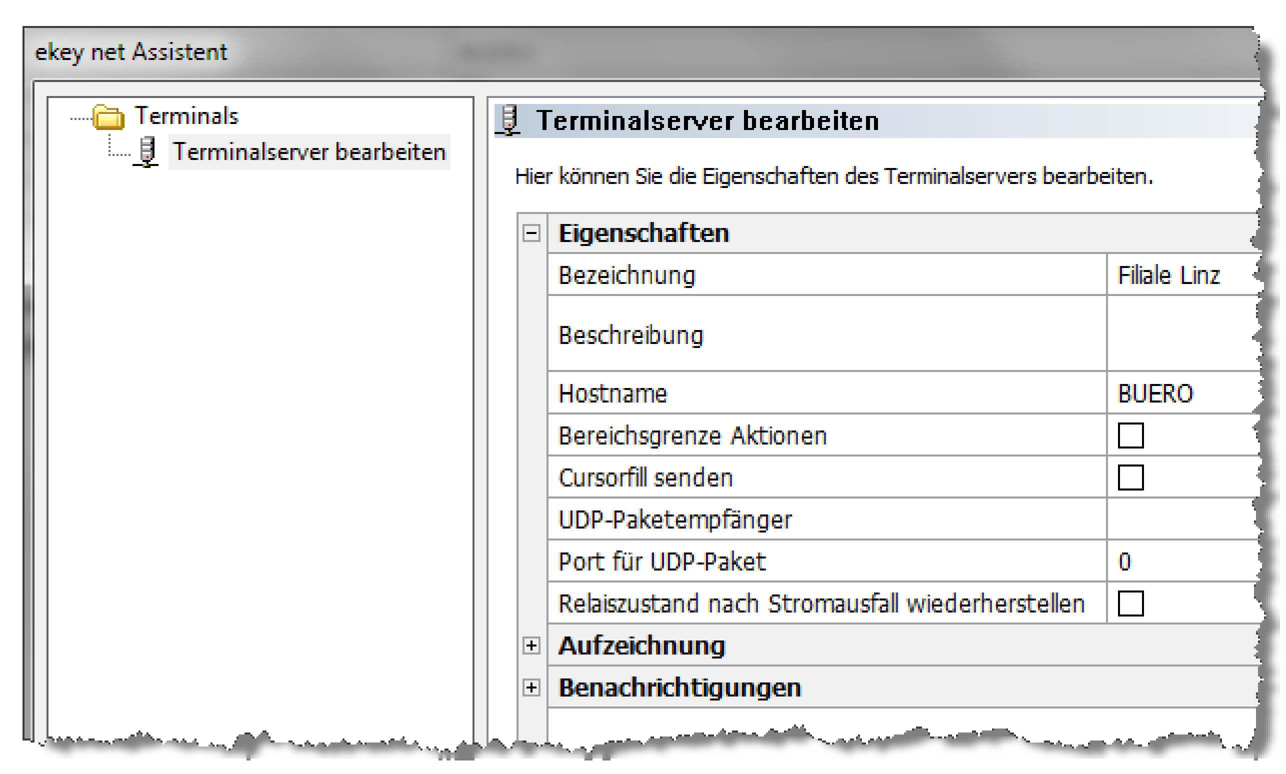
Bereichsgrenze Aktionen:

Bereichsgrenze Aktionen	☐

Terminalgruppe als Bereichsgrenze aktivieren. Informationen zur Funktion und Wirkungsweise von Bereichsgrenzen finden Sie im Kapitel 16.

6.6.3.1.2 Konfiguration der Terminalgruppe „ekey net Terminalserver"

Wählen Sie den für die Konfiguration gewünschten ekey net Terminalserver aus.



Unter**Eigenschaften** können die entsprechenden Konfigurationenvorgenommen werden.

Die ekey net Terminalserver bieten eine Reihe von Zusatzfunktionen, die über den reinen Zutritt hinausgehen. Speziell sind die Optionen hinsichtlich **Benachrichtigung** und **Aufzeichnung** zu nennen.

Folgende Parameter können Sie beim ekey net Terminalserver einstellen:

Bezeichnung:

Bezeichnung	Eingangstüren

Bezeichnung (Name) des ekey net Terminalservers. Diese Bezeichnung wird auch im Terminalexplorer angezeigt.

Beschreibung:

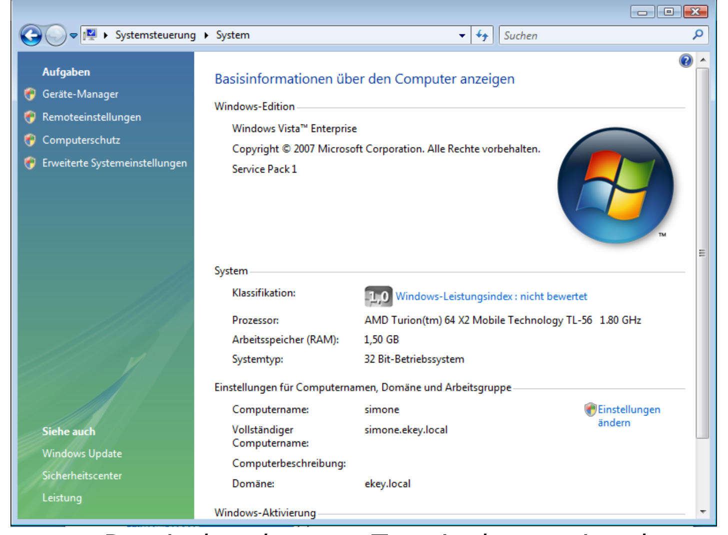
Beschreibung	

Freies Beschreibungsfeld für Informationen zu der Terminalgruppe

Hostname:

Hostname	

Der Name des Rechners auf dem der gewählte ekey net Terminalserver läuft, ist hier einzutragen. Der Name ist in der „Windows Systemsteuerung" -> „System" zu finden.





Damit der ekey net Terminalserver im ekey net korrektarbeitet, muss unbedingt der Rechner vom Masterserver ausgehend über das IP - Netzwerk über den Servernamen(DNS) erreichbar sein (pingbar) und umgekehrt. Eine Erreichbarkeitnur über die IP-Adresse reicht nicht aus! Achtung nur den Hostnamen (ohne Punkt am Ende) ohne Domain
*„**Hostname~~.local~~**"*

Bereichsgrenze Aktionen:

Bereichsgrenze Aktionen	☐

Hier wird definiert, ob der gewählte Terminalserver eine Bereichsgrenze darstellt. Informationen zum Thema Bereichsgrenzen finden Sie im Kapitel 16

Cursorfill senden:

Cursorfill senden	☐

Der ekey net Terminalserver kann hier dazu veranlasst werden, ein Cursorfill bei einem positiven Zutritt zu senden. Cursorfill heißt, dass an der Cursorpostion einer fremden Anwendung (z.B. Excel usw.) ein Texteintrag gemacht wird (ekey net simuliert hier eine Tastatureingabe). Dazu müssen 2 Bedingungen erfüllt sein.

- Die Anwendung in der der Eintrag gemacht werden soll, läuft am gleichen Rechner wie der gewählte Terminalserver.
- Die Anwendung „**ekey Cursorfill**" ist am gleichen Rechner installiert. Diese Anwendung ist über das ekey net –Setup installierbar.

UDP-Paketempfänger & Port für UDP-Paket:

UDP-Paketempfänger	
Port für UDP-Paket	0

ekey net Terminalserver können bei einem positiven Match ein UDP-Paket an eine hier definierbare IP-Adresse über den definierbaren Port senden. Der Inhalt dieses Datenpaketes ist vordefiniert und kann nicht verändert werden. Den Paketaufbau sehen Sie unter Kapitel 19.1

Relaiszustand nach Stromausfall

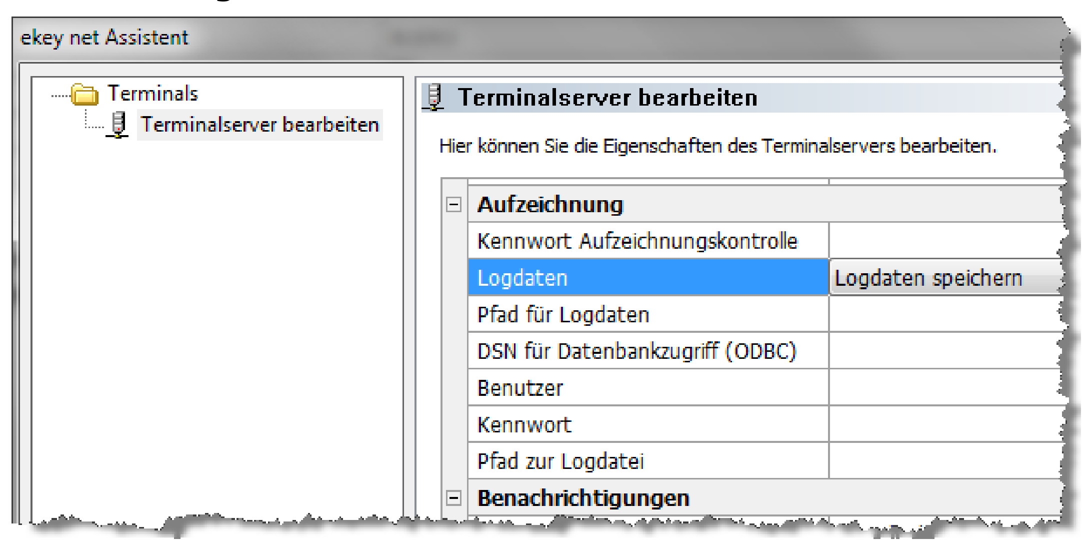
Relaiszustand nach Stromausfall wiederherstellen	☐

Kommt es zu einem Stromausfall an den ekey net SE, so fallen natürlich die aktiven Relais ab. In der Standardkonfiguration ist es so, dass nach Wiederkehr der Spannung die Relais abgefallen bleiben, bis eben ein neues Ereignis dies wieder aufhebt. Wählt man diese Checkbox, so merkt sich der ekey net Terminalserver die Relaiszustände der einzelnen ekey net SE und setzt Sie nach Wiederkehr der Spannungsversorgung alle auf den Status,den Sie vor dem Stromausfall hatten. Dies allerdings nur, wenn das Relais über eine Dauerschaltung aktiviert wurde. (= Aktion „Anschluss X ein")

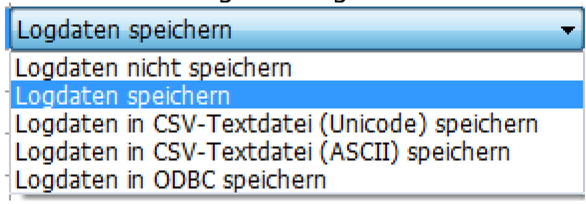


Diese Einstellung ist wirkungslos bei Relais, die über die Selbsthaltungsfunktion dauerhaft bis zu einem definierten Zeitpunkt aktiviert wurden! In diesem Fall bleibt auch das Relais nach Spannungswiederkehr ausgeschalten! Weiters ist diese Funktion bei den Modellen „REL" nicht möglich!

Aufzeichnung:



Die Aufzeichnung von Logdaten in verschiedenen Formaten ist hier zu konfigurieren.



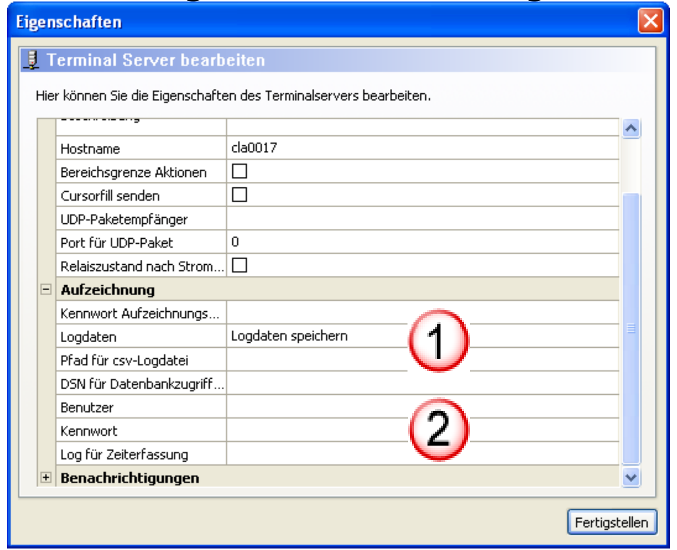
Näheres zum Datenlogging finden Sie im Kapitel 15.

Kennwort Aufzeichnungskontrolle:

Kennwort Aufzeichnungskontrolle	

Sie können ein Kennwort für die Aufzeichnungskontrolle in den **„Optionen"->"Aufzeichnung"** festlegen (siehe Kapitel 8.1.7). Haben Sie dies definiert, so müssen Sie dieses Passwort hier eingeben um Änderungen vornehmen zu können.

Pfad für Logdaten – Pfad zur Logdatei – Unterschied!



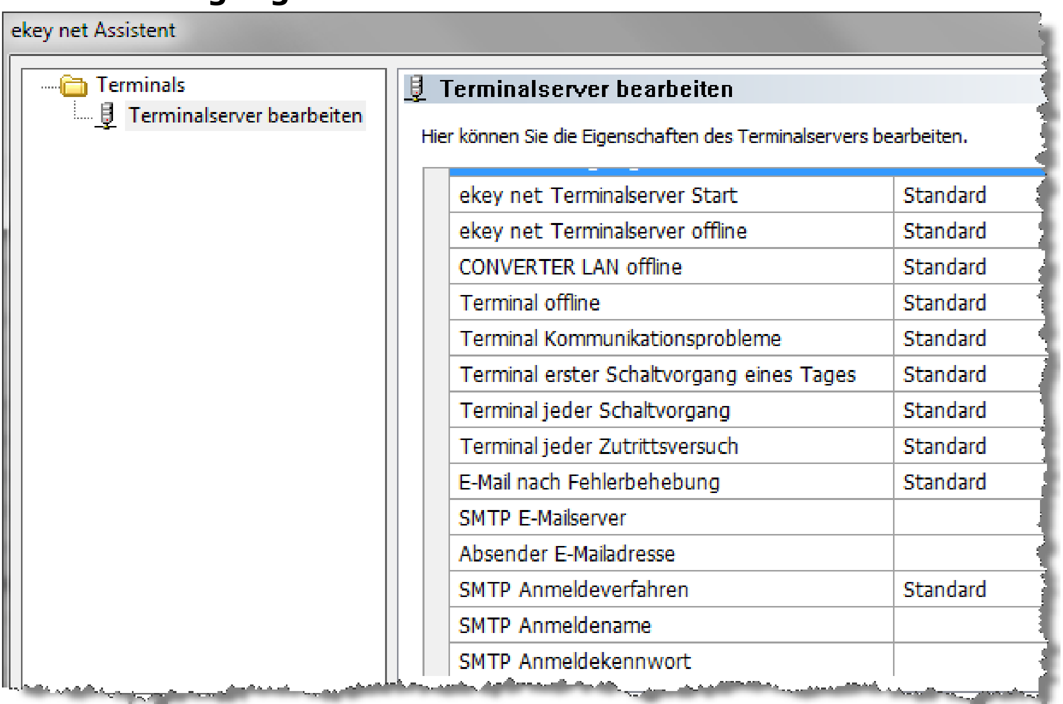
Unterscheiden Sie bitte die Bedeutung der beiden **„Log – Dateien"**:

1 Wenn in eine .CSV (Textdatei) aufzeichnen, so werden alle Informationen, gemäß der Konfiguration im Menü **„Optionen"->"Aufzeichnung"**, in diese Datei geschrieben

2 Möchten Sie zur einfacheren Auswertung – speziell für Zeiterfassungssysteme – nur positive Matches mit vordefinierten Benutzerinformationen aufzeichnen, dann definieren Sie einen **„Pfad zurLogdatei**.

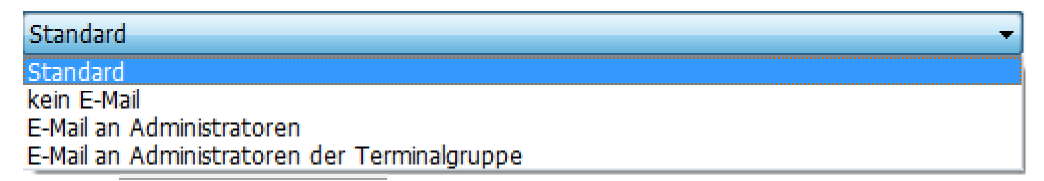
Sie müssen abschließend noch bei jedem **ekey net FS** definieren, ob Sie dessen Daten mitloggen wollen. Aktivieren Sie dazu in den Eigenschaften des Fingerscanners die Checkbox: positive Matchingeinträge im Log ☑

Benachrichtigungen:



Bei Zuständen oder Ereignissen die am ekey net Terminalserver auftreten, können Nachrichten in folgenden Formen an definierte Empfänger abgesetzt werden:





- Standard Hier gilt die Einstellung, die im Bereich der Grundeinstellungen/ Optionen für die Benachrichtigung gemacht wurde.Wählen Sie bei allen ekey net Terminalservern „Standard", so können Sie Änderungen der Benachrichtigungsfunktion zentral im Bereich „Optionen" durchführen. Siehe dazu auch Kapitel 8.1.1
- kein E-Mail Für diesen ekey net Terminalserver wird bei dem auftretenden Ereignis keine Benachrichtigung gesandt.
- E-Mail an Administratoren Bei dem auftretenden Ereignis wird ein E-mail an alle ekey net Administratoren des Systems gesandt.
- E-Mail an Administratoren der Terminalgruppe Bei dem auftretenden Ereignis wird ein Email nur an die für diesen Terminalserver berechtigten ekey net Administratoren gesandt.

Für die Versendung der Benachrichtigungen sind Einstellungenabhängig ihrer System- und Serverarchitektur vorzunehmen:

SMTP E-Mailserver	

Hostname oder Adresse des Postausgangs – Servers hier eintragen

Absender E-Mailadresse	

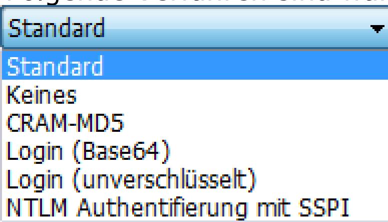
Die Emailadresse des Absenders, in diesem Fall von ekey net ist hier zu definieren. (fiktive Adresse)

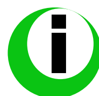


Sie können an ekey net kein Email senden! Die hier eingegebene Adresse hilft ihnen, wenn Sie eine für sich sprechende Adresse wählen,in ihrem Posteingangsordner klar zu erkennen, von wem die Email kommt.

SMTP Anmeldeverfahren	Keines

Wählen Sie das korrekte Verschlüsselungsverfahren Ihres SMTP - Servers aus
Folgende Verfahren sind wählbar:





Die Einstellungen für die Emailfunktionen, speziell im Hinblick auf den SMTP –Server sind abhängig von ihrer Systemkonfiguration. Ekey kann ihnen in diesem Bereich nureingeschränkt Unterstützung bieten. Wenn Sie diese Funktionen aktivieren möchten, ziehen Sie bitte ihre IT-Spezialisten für die Konfiguration zu Rate.



SMTP Anmeldename

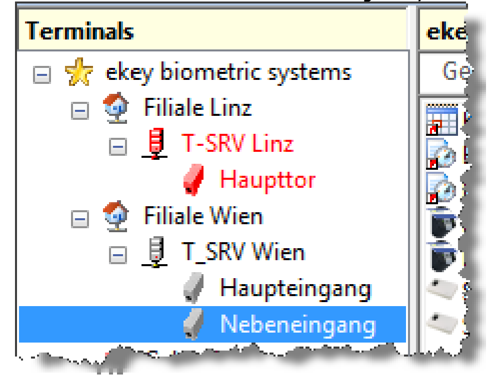
Wenn erforderlich - bei den meisten SMTP Servern kann dieses Feld leer bleiben.

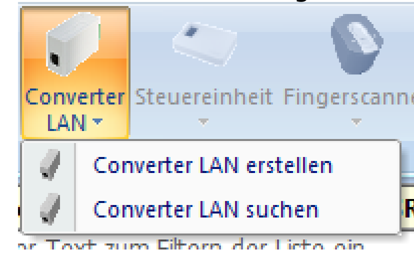
SMTP Anmeldekennwort

Wenn erforderlich - bei den meisten SMTP Servern kann dieses Feld leer bleiben.

6.6.3.1.3 Konfigurieren der Terminalgruppe „ekey net CV LAN"

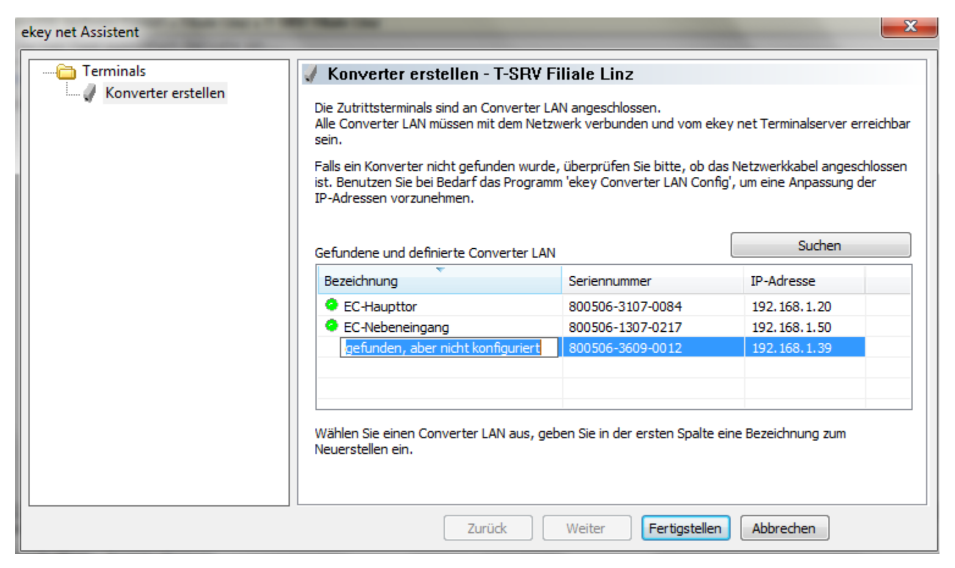
Wählen Sie in der Terminalstruktur den für die Konfiguration gewünschten ekey net CV LAN aus und öffnen Sie das Objekt, oder starten Sie zur Neuanlage den ekey net Assistent.





6.6.3.1.3.1 ekey net CV LAN ist ONLINE:

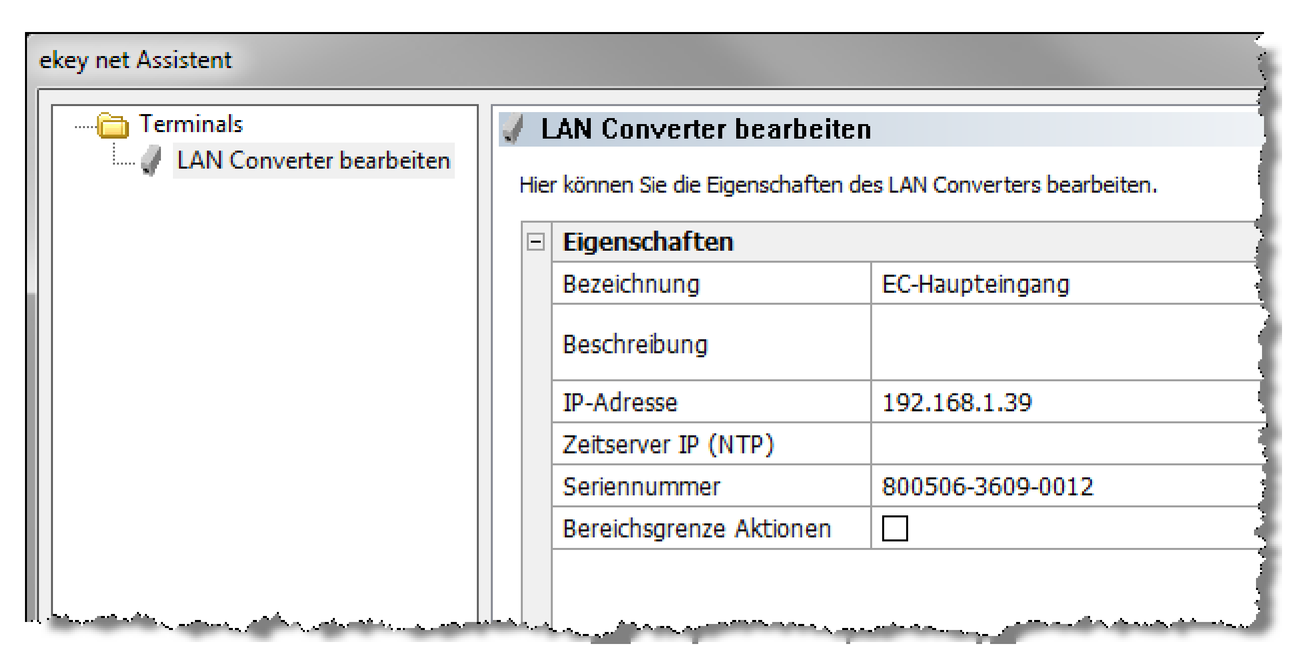
Klicken Sie bitte auf **„Converter LAN suchen"**



Wählen Sie den neuen ekey net CV LAN durch **2 Klicks** auf das Bezeichnungsfeld und vergeben Sie einen aussagekräftigen Namen. Mit einem Klick auf „Fertigstellen" übernehmen Sie die Konfiguration und der ekey net CV LAN geht ONLINE.

6.6.3.1.3.2 ekey net CV LANist OFFLINE oder noch nicht im System montiert:

Klicken Sie bitte auf **„Converter LAN erstellen“**



In den Eigenschaften des ekey net CV LAN können folgende Parameter definiert werden.

Bezeichnung:

Bezeichnung	Haupteingangstüren

Bezeichnung des ekey net CV LAN. Vergeben Sie hier einen entsprechenden Namen. Die Bezeichnung wird dann in den Geräte-Explorer übernommen.

Beschreibung

Beschreibung	

Freies Beschreibungsfeld, in dem Sie Informationen zum Gerät festhalten können.

IP-Adresse

IP-Adresse	192.168.1.39

IP-Adresse des ekey net CV LAN. Die richtige IP-Adresse müssen Sie mit dem Programm



konfigurieren. Sehen Sie dazu auch Kapitel 5.2.3.2

Zeitserver IP (NTP)

Zeitserver IP (NTP)	

Hier definieren Sie die IP-Adresse eines NTP-Zeitservers.NTP (Network Time Protocol) ist ein Standard zur Synchronisierung von Uhren im Netzwerk. Die Konfiguration eines NTP-Servers am ekey net CV LAN ermöglicht im Offline-Zustand(keine Verbindung zum ekey net Terminalserver) eine genaue Zeit an den Geräten (ekey net FS). Dies führt wiederum dazu,

dass im Offlinezustand die Zutritte uneingeschränkt möglich sind, sofern der NTP-Server über den ekey net CV LAN erreichbar ist.

Die ekey net FS haben keine Echtzeituhr implementiert, die auch über einen Spannungsausfall hinaus die genaue Zeitmessung garantieren würde. Verliert der Fingerscanner die Zeit (durch Spannungsausfall), so wird nur mehr Benutzern (Fingern) Zutritt gewährt, die dem Zeitfenster „**Immer**" zugeordnet sind. Benutzer mit eingeschränktem zeitlichen Zutritt erhalten solange keine Freischaltung, bis die Zeit am Fingerscanner wieder aktualisiert ist. Diese Aktualisierung erfolgt entweder durch

- den NTP-Server und ekey net CV LAN.
- den ekey net Terminalserver.



Achten Sie darauf, dass Sie den ekey net CV LAN netzwerktechnisch richtig konfigurieren. Gateway und Netzmaske müssen richtig definiert werden, damit Sie den NTP-Server erreichen und die Funktion ordentlich arbeitet. Gehen Sie bei der Konfiguration des ekey net CV LAN nach Kapitel5.2.3vor. Für die Netzwerkeinstellungen sprechen Sie bitte mit Ihrem Systemadministrator.

<u>Seriennummer:</u>

Seriennummer	800506-3609-0012

Die Seriennummer ist die eindeutige Identifizierung des Gerätes. Bei manueller Konfiguration ist die korrekte Eingabe essentiell wichtig!

<u>Bereichsgrenze Aktionen:</u>

Bereichsgrenze Aktionen	☐

Hier definieren Sie, ob der ekey net CV LAN eine Bereichsgrenze darstellt. Die Funktionen und Möglichkeiten von Bereichsgrenzen sehen Sie im Kapitel 16

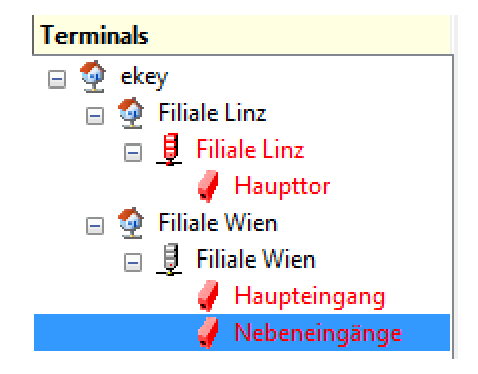
6.6.3.2 Anlegen der Geräte (Terminals)

Unter Geräten versteht man
- ekey net FS
- ekey net SE
- ekey net Verbund SE
- ekey net CV WIEG

Anhand der von Ihnen erstellten und verkabelten Architektur ihres Systems (siehe auch unter Kapitel 6.6.1) können Sie nun die Geräte anlegen. Wählen Sie dazu nun in der Terminalstruktur den ekey net CV LANunter dem Sie entsprechende Geräte (Fingerscanner und SE) anlegen möchten.

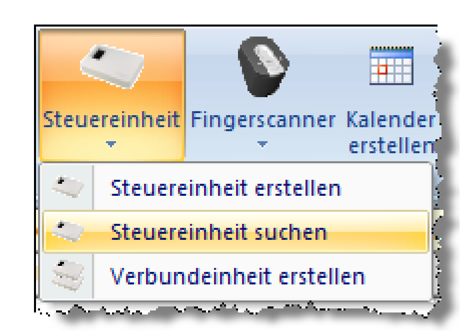
6.6.3.2.1 <u>Anlage ekey net SE</u>

Wählen Sie dazu nun in der Terminalstruktur den, lt. Architektur, richtigenekey net CV LAN für die Geräteanlage:

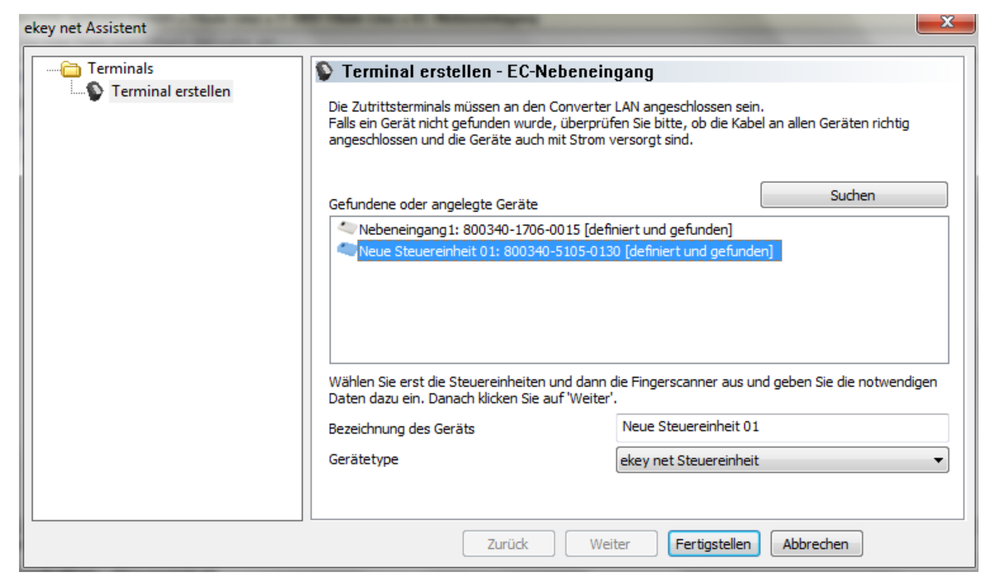




6.6.3.2.1.1 Steuereinheit ONLINE im System



Wählen Sie„**Steuereinheit suchen**"

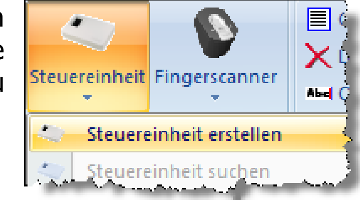


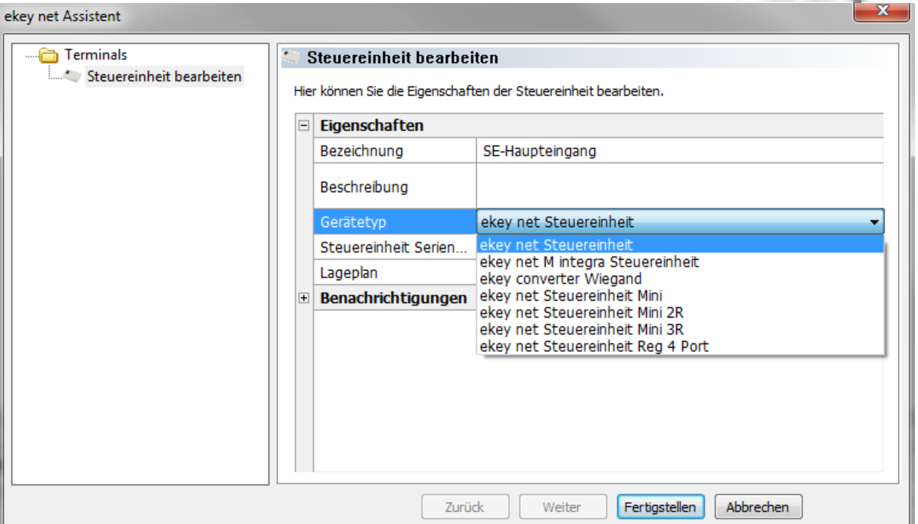
Füllen Sie unter **„Bezeichnung .."** einen Gerätenamen aus und klicken Sie auf **„Fertigstellen"**

Die neue Steuereinheit geht online.

6.6.3.2.1.2 Steuereinheit OFFLINE oder noch nicht im System montiert:

Sollten Sie Hardwarekomponenten noch nicht installiert haben, so können Sie diese auch offline vorbereiten. Klicken Sie dazu bitte auf **„Steuereinheit erstellen"**





Wählen Sie bitte den entsprechenden **Gerätetyp**, verwenden Sie dann eine aussagekräftige **Bezeichnung** und tragen Sie die richtige **Seriennummer** der Steuereineheit ein



Die Seriennummer finden Sie auf einer Etikette am Gerät. Sie ist 14-stellig und beginnt mit 8 (z.B. 800340 2209 0001).



Die Eingabe der Seriennummer ist unbedingt notwendig! Die Geräte werden an Hand der Seriennummer im System identifiziert. Geben Sie keine Seriennummer ein, wird das Gerät nicht erkannt und die Funktion des Gerätes ist nicht gegeben!

Bezeichnung:

Bezeichnung	SE HAUPT

Geben Sie hier eine sprechende Bezeichnung für die ekey net SE ein. Die Bezeichnung wird dann auch im Terminalexplorer und im Gerätestatus angezeigt.

Beschreibung:

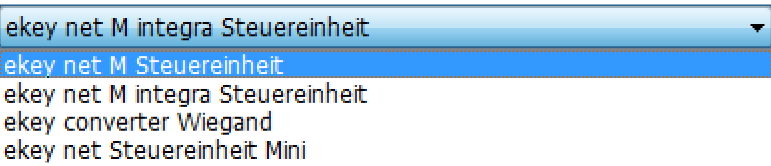
Beschreibung	

Freies Feld für zusätzliche Informationen zur ekey net SE

Gerätetyp:

Gerätetyp	ekey net M integra Steuereinheit

Der Gerätetyp sollte, nachdem Sie im Menü bereits den Richtigen gewählt haben stimmen. Sollten Sie hier aber den falschen sehen, können Sie hier die richtige Type wählen (speziell, wenn die Steuereinheit automatisch angelegt wurde, ist hier die Type zu kontrollieren)

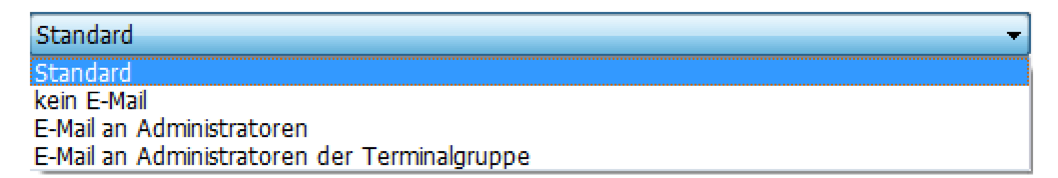


In der Liste der Combo-Box sehen Sie alle im System definierten Typen von Steuereinheiten und auch die kundenspezifisch generierten Gerätetypen (siehe Kapitel 8.1.4.1) werden hier gelistet.

Benachrichtigungen:

Benachrichtigungen

Bei Zuständen oder Ereignissen, die an ekey net SE auftreten, können Nachrichten in folgenden Formen an definierte Empfänger abgesetzt werden:



- Standard hier gilt die Einstellung, die im Bereich der Grundeinstellungen / Optionen für die Benachrichtigung gemacht wurde.Wählen Sie bei allen ekey net SE „Standard", so können Sie Änderungen der Benachrichtigungsfunktion zentral im Bereich „Optionen" durchführen. Siehe dazu auch Kapitel 8.1.1
- kein E-Mail für diese ekey net SE wird bei dem auftretenden Ereignis keine Benachrichtigung gesandt.
- E-Mail an Administratoren Bei dem auftretenden Ereignis wird ein E-mail an alle Administratoren des Systems gesandt.
- E-Mail an Administratoren der Terminalgruppe Bei dem auftretenden Ereignis wird nur ein E-Mail an die für diesen Terminalserver berechtigten Administratoren gesandt.

Folgende Ereignisse können im Bereich des ekey net SE zuBenachrichtigungen führen:

Terminal offline	Standard
E-Mail nach Fehlerbehebung	Standard
SMTP E-Mailserver	
Absender E-Mailadresse	
SMTP Anmeldeverfahren	Standard
SMTP Anmeldename	
SMTP Anmeldekennwort	

Für die Versendung der Benachrichtigungen sind Einstellungen abhängig von ihrer System- und Serverarchitektur vorzunehmen:

SMTP E-Mailserver	

Hostname oder Adresse des Postausgangs – Servers hier eintragen

Absender E-Mailadresse	

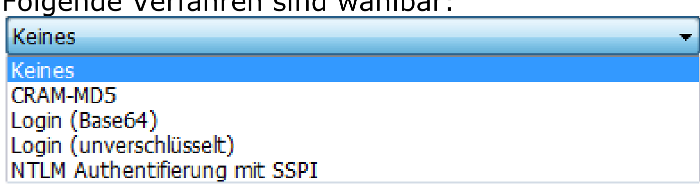
Die Emailadresse des Absenders, in diesem Fall von ekey net ist hier zu definieren.

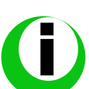


Sie können an ekey net kein E-mail senden! Die hier eingegebene Adresse hilft ihnen, wenn Sie eine für sich sprechende Adresse wählen,in ihrem Posteingangsordner klar zu erkennen, von wem die E-mail kommt.

SMTP Anmeldeverfahren	Keines

Wählen Sie das korrekte Verschlüsselungsverfahren Ihres SMTP - Servers aus
Folgende Verfahren sind wählbar:





Die Einstellungen für die E-Mail Funktionen, speziell im Hinblick auf den SMTP –Server sind abhängig von ihrer Systemkonfiguration. ekey kann ihnen in diesem Bereich nureingeschränkt Unterstützung bieten. Wenn Sie diese Funktionen aktivieren möchten, ziehen Sie bitte ihre IT-Spezialisten für die Konfiguration zu Rate.

SMTP Anmeldename	

Wenn erforderlich - bei den meisten SMTP Servern kann dieses Feld leer bleiben.



SMTP Anmeldekennwort	

Wenn erforderlich - bei den meisten SMTP Servern kann dieses Feld leer bleiben.

6.6.3.2.2 Anlage ekey net Verbundsteuereinheiten

Mithilfe einer**ekey net Verbundsteuereinheit** kann die Anzahl der schaltbaren Relais von bis zu max. 4 Relais auf 1 ekey net SE (Variiert je nach Modell von 1 bis 4) auf bis zu **max. 28** Relais mit 7 ekey net SE im Verbund erhöht werden.

Verbundsteuereinheiten sind ausschließlich dazu gedacht, an **1 ekey net CV LAN 1** Verbundsteuereinheit zu betreiben zb. Liftsteuerung (nicht mehrere)!

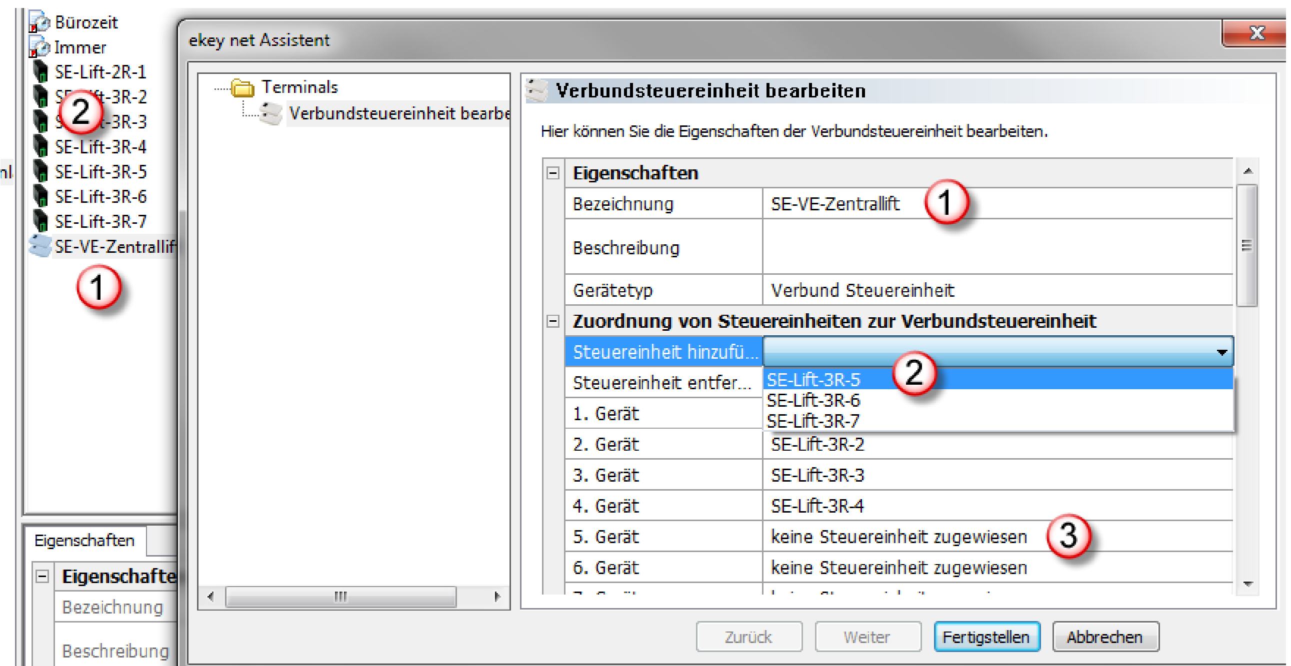
folgendes muss eingehalten werden:
1.) Keines dieser Geräte am Bus (weder Steuereinheit noch Fingerscanner) darf ein benutzerdefiniertes Gerät sein.
2.) Als zugeordnete Ereignisse dürfen nur die vordefinierten Verbund-Ereignisse verwendet werden und keine Benutzerdefinierten oder Doppelrelaisfunktionen.



*Detaillierte Informationen zur vorbereitenden Konfiguration und dem Funktionsprinzip finden Sie im **Kapitel6.6.3.2.2 „ekey net Verbundsteuereinheit".***

Wählen Sie **„Verbundeinheit erstellen"**







Wählen Sie eine aussagekräftige Bezeichnung für dieVerbundsteuereinheit. Dieser wird auch im Gerätefenster angezeigt und durch ein spezielles Symbol gekennzeichnet



Wählen Sie die nächste verfügbare ekey net SE für den Verbund aus



Diese wir automatisch an die nächste freie Gerätestelle gereiht



*Zur besseren Übersicht empfehlen wir eine Numerierung der einzelnen ekey net SE wie im **Kapitel 12.1.2 „Vorbereitende Konfigurationsschritte"**beschrieben*

Nach erfolgter Konfiguration können Sie die Zuordnung der einzelnen Relais im Eigenschaftsfenster unter **„Relaiskonfiguration"** überprüfen.

Terminals

- ekey biometric systems GmbH
  - Filiale Linz
  - Filiale Wien
    - T-SRV Filiale Wien
      - EC-Haupteingang
      - EC-Haupttor
      - EC-Nebeneingang
      - Zentralliftanlage
        - EC-Zentralliftanl
- Deleted

ekey biometric systems GmbH » Filiale Wien » T-SRV Filiale Wien » Zentralliftanlage » EC-Zentralliftanlage

Geben Sie hier Text zum Filtern der Liste ein...

Kalender Österreich, Bürozeit, Immer, SE-Lift-2R-1, SE-Lift-3R-2, SE-Lift-3R-3, SE-Lift-3R-4, SE-Lift-3R-5, SE-Lift-3R-6, SE-Lift-3R-7, SE-VE-Zentrallift

Eigenschaften

Steuereinheit entfernen	
1. Gerät	SE-Lift-2R-1
2. Gerät	SE-Lift-3R-2
3. Gerät	SE-Lift-3R-3
4. Gerät	SE-Lift-3R-4
5. Gerät	SE-Lift-3R-5
6. Gerät	SE-Lift-3R-6
7. Gerät	SE-Lift-3R-7
Relaiskonfiguration	
01. "SE-Lift-2R-1" Relais: 1	Verbund SE Anschluss 1 schalten
02. "SE-Lift-2R-1" Relais: 2	Verbund SE Anschluss 2 schalten
03. "SE-Lift-3R-2" Relais: 1	Verbund SE Anschluss 3 schalten
04. "SE-Lift-3R-2" Relais: 2	Verbund SE Anschluss 4 schalten
05. "SE-Lift-3R-2" Relais: 3	Verbund SE Anschluss 5 schalten
06. "SE-Lift-3R-3" Relais: 1	Verbund SE Anschluss 6 schalten
07. "SE-Lift-3R-3" Relais: 2	Verbund SE Anschluss 7 schalten
08. "SE-Lift-3R-3" Relais: 3	Verbund SE Anschluss 8 schalten
09. "SE-Lift-3R-4" Relais: 1	Verbund SE Anschluss 9 schalten
10. "SE-Lift-3R-4" Relais: 2	Verbund SE Anschluss 10 schalten
11. "SE-Lift-3R-4" Relais: 3	Verbund SE Anschluss 11 schalten
12. "SE-Lift-3R-5" Relais: 1	Verbund SE Anschluss 12 schalten
13. "SE-Lift-3R-5" Relais: 2	Verbund SE Anschluss 13 schalten
14. "SE-Lift-3R-5" Relais: 3	Verbund SE Anschluss 14 schalten
15. "SE-Lift-3R-6" Relais: 1	Verbund SE Anschluss 15 schalten
16. "SE-Lift-3R-6" Relais: 2	Verbund SE Anschluss 16 schalten
17. "SE-Lift-3R-6" Relais: 3	Verbund SE Anschluss 17 schalten
18. "SE-Lift-3R-7" Relais: 1	Verbund SE Anschluss 18 schalten
19. "SE-Lift-3R-7" Relais: 2	Verbund SE Anschluss 19 schalten
20. "SE-Lift-3R-7" Relais: 3	Verbund SE Anschluss 20 schalten



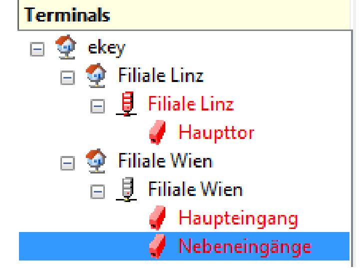
Eine nachträgliche Änderung der Zuordnung ist nur durch LÖSCHEN der ekey net Verbundsteuereinheit, NEUERSTELLUNG und NEUE ZUORDNUNG der verfügbaren ekey net SE möglich!

6.6.3.2.3 Anlage ekey net FS

Bevor Sie mit der Geräteanlage starten, müssen Sie wissen,
- *welche Gerätetype (S,M,L, AP, integra, RFID,….)*
- *mit welcher Seriennummer*

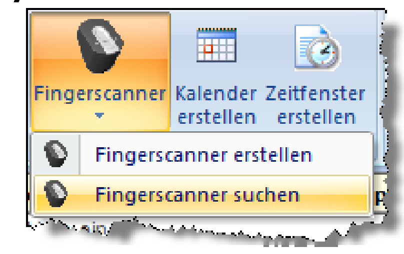
welchem ekey net CV LAN zugeordnet (verkabelt) ist. Sie finden die Daten auf den Seriennummernetiketten der einzelnen Geräte.

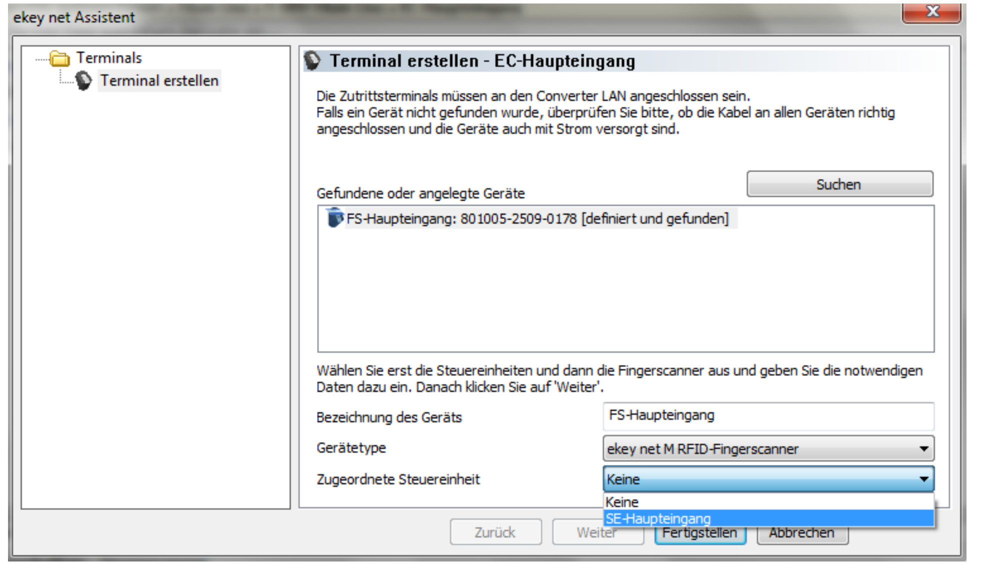
Wählen Sie dazu nun in der Terminalstruktur den ekey net CV LAN für die Geräteanlage.



6.6.3.2.3.1 **Fingerscanner ONLINE im System**

Wählen Sie **„Fingerscanner suchen“**





Füllen Sie unter **„Bezeichnung ..“** einen Gerätenamen aus und klicken Sie auf **„Fertigstellen“**



Ordnen Sie dem Fingerscanner die ekey net SE zu, auf der durch Ereignisse (z.B. mit Finger Türe öffnen) definierte Aktionen ausgeführt werden. Jedem ekey net FS kann eine ekey net SE zugeordnet werden.

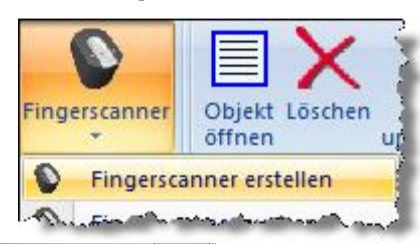
Der neue Fingerscanner geht online.

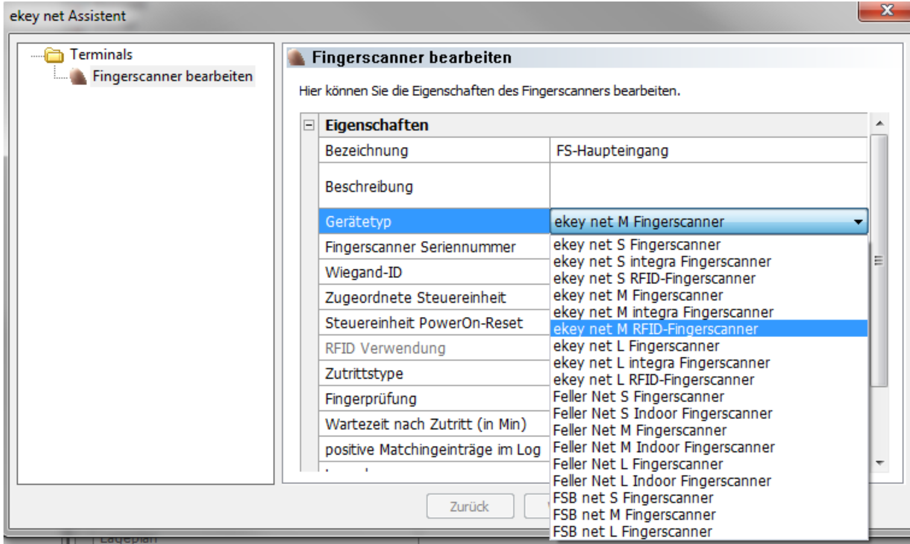


Bei Erstellung eines Fingerscanners über die Funktion **„Fingerscanner suchen“**wird**KEINE Steuereinheit automatisch** angelegt!

6.6.3.2.3.2 Fingerscanner OFFLINE oder noch nicht im System montiert:

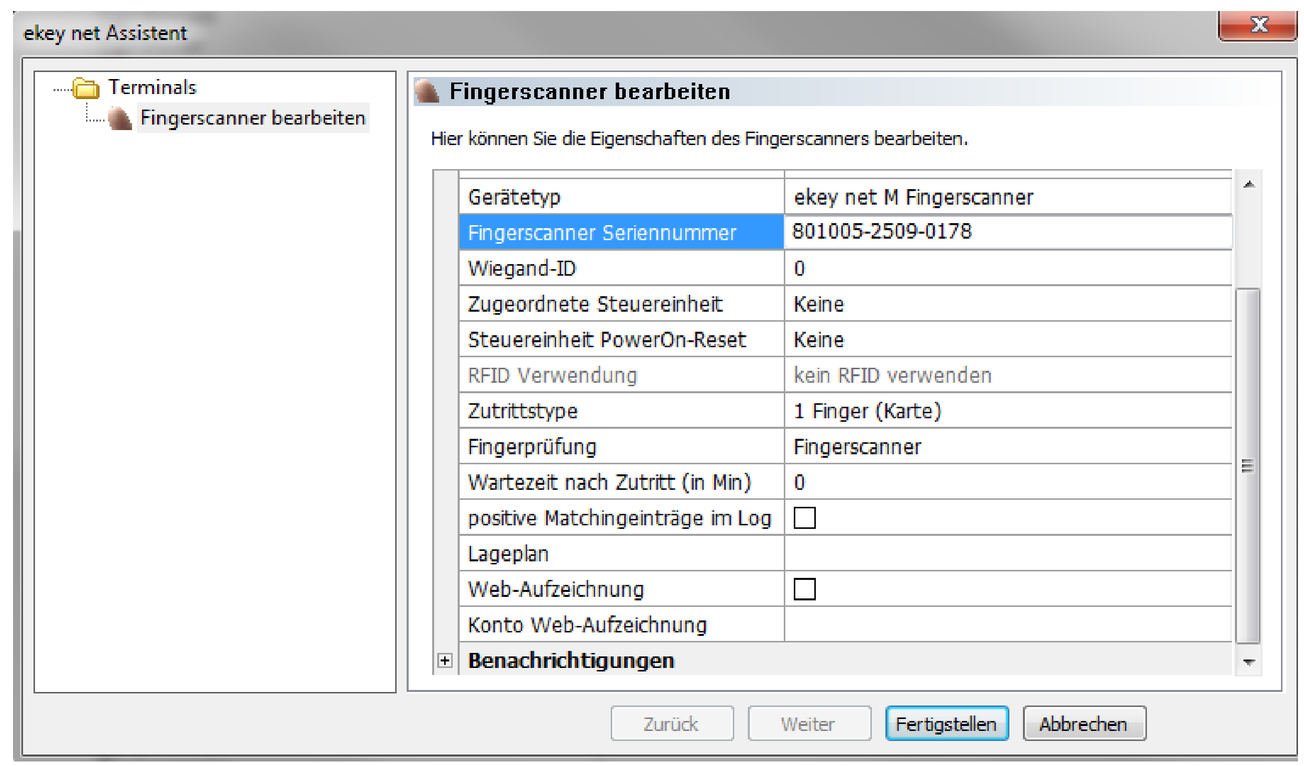
Sollten Sie Hardwarekomponenten noch nicht installiert haben, so können Sie diese auch offline vorbereiten. Klicken Sie dazu bitte auf **„Fingerscanner erstellen"**





Wählen Sie bitte den entsprechenden **Gerätetyp**, verwenden Sie dann eine aussage-kräftige **Bezeichnung** und tragen Sie die richtige **Seriennummer** desFingerscanners ein

Die Seriennummer finden Sie auf einer Etikette am Gerät. Sie ist 14-stellig und beginnt mit 8



Folgende Einstellungen sind hier zu tätigen:

Bezeichnung:

Bezeichnung	FS NEBEN 1

Hier definieren Sie die Bezeichnung des ekey net FS. Diese Bezeichnung wird dann auch im Terminalexplorer (=Geräteübersichtsfenster) angezeigt und sollte so gewählt werden, dass eine eindeutige Zuordnung zur jeweiligen Tür gegeben ist.

Beschreibung

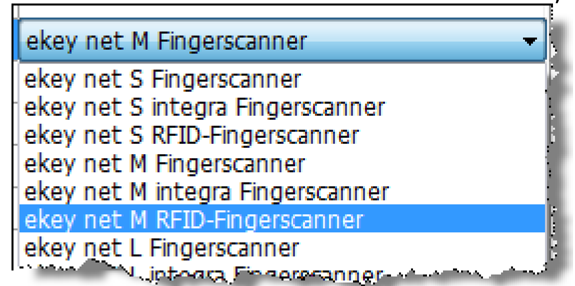
Beschreibung	

Freies Eingabefeld für weitere Informationen zum Fingerscanner

Gerätetyp:

Gerätetyp	ekey net M Fingerscanner

Der Gerätetyp sollte, nachdem Sie im Menü den richtigen gewählt haben, bereits stimmen. Sollten Sie hier aber den Falschen sehen, können Sie hier zur richtigen Type korrigieren.



In der Liste der Combo-Box sehen Sie alle im System definierten Typen von Fingerscannern und auch die kundenspezifisch generierten Gerätetypen (siehe Kapitel 8.1.4.1) werden hier gelistet.

Fingerscanner Seriennummer:

Fingerscanner Seriennummer	000000-0000-0000

Hier ist die Seriennummer des ekey net FSs einzugeben. Die Seriennummer finden Sie auf einer Etikette am Gerät. Sie ist 14-stellig und beginnt mit 8. (z.B. 800321 2209 0003)



Die Eingabe der Seriennummer ist unbedingt notwendig! Die Geräte werden an Hand der Seriennummer im System identifiziert. Geben Sie keine Seriennummer ein, wird das Gerät nicht erkannt und die Funktion des Gerätes ist nicht gegeben!

Wiegand ID:

Wiegand-ID	0

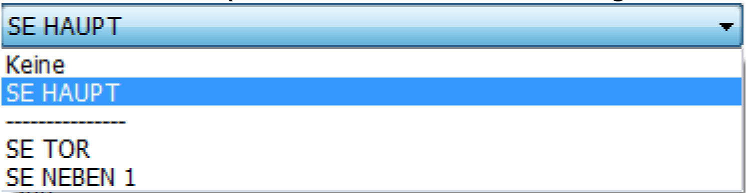
Die Wiegand ID ist nur einzugeben, wenn Sie Zugangsdaten über einen ekey converter Wiegand an ein Wiegand-System versenden wollen(siehe Kapitel 13).

Zugeordnete Steuereinheit:

Zugeordnete Steuereinheit	SE NEBEN 1

Hier ordnen Sie dem Fingerscanner die ekey net SE zu, auf der durch Ereignisse (z.B. mit Finger Türe öffnen) definierte Aktionen ausgeführt werden. Jedem ekey net FS kann eine Steuereinheit zugeordnet werden.

Damit ist auch definiert, dass mit einem ekey net FS maximal 4 Aktoren (Relais) geschalten werden können. (Ausnahme Bereichsschaltung -> siehe Kapitel 16)



Öffnen Sie die Liste der Combobox, so sehen Sie alle ekey net SE in ihrem System gelistet.
Die strichlierte Linie --------------- teilt die ekey net SE in jene

- die im gleichen Bussegment wie der gewählte Fingerscanner ist (am gleichen ekey net CV LAN elektrisch angebunden ist) -> oberhalb der Linie
- die in einem anderen Bussegment angebunden sind (an einem anderen ekey net CV LAN als der Fingerscanner). -> unterhalb der Linie

Grundsätzlich kann jede im System vorhandene Aktoreinheit (ekey net SE) zu einem ekey net FS zugeordnet werden.

Allerdings ist bei Aktoreinheiten, die nicht im gleichen Bussegment liegen (also unterhalb der strichlierten Linie gelistet sind), der Offline-Betrieb (ekey net Terminalserver nicht aktiv bzw. von ekey net CV LAN getrennt) nicht gegeben!



Achten Sie also für die einwandfreie Funktion des Offline-Betriebes hier unbedingt auf die Verkabelung und Zuweisung der Geräte!

Steuereinheit PowerOn Reset:

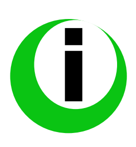
Steuereinheit PowerOn-Reset	SE HAUPT

Auf jeder ekey net SE ist die Spannungsversorgung für die ekey net FS (PIN 3 und 4) schaltbar ausgeführt. Das heißt, dass die Versorgungspannung für die Fingerscanner abgeschalten werden kann und der Fingerscanner stromlos wird.

Ausgelöst wird diese Abschaltung der Versorgungsspannung für etwa 3 Sekunden durch den ekey net Terminalserver dann, wenn der ekey net FS für einen definierten Zeitraum von 2 min nicht mehr meldet (Überwachungsfunktion).
Die ekey net SE, die die Abschaltung vornimmt, definieren Sie hier.



Sie müssen natürlich den ekey net FS auch über PIN 3 und 4 der hier gewählten Steuereinheit entsprechend versorgen.
Weiters ist hier nur eine ekey net SE definierbar, die im gleichen Bussegment wie der ekey net FS liegt.

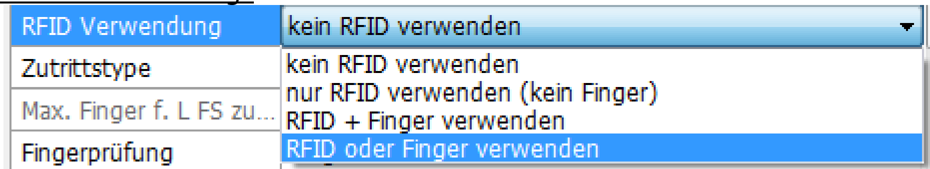


Die ekey net FS entsprechen den geltenden Normen der elektromagnetischen Verträglichkeit. Es gibt aber im Feld Bedingungen speziell hinsichtlich ESD, die Belastungen am Scanner hervorrufen, die zum Absturz des Systems führen. Mit dieser Funktion kann die Ausfallsicherheit des Scanners gegen ESD massiv erhöht werden.



*Sollte es zu extremen ESD Störungen kommen und können diese nicht eingedämmt werden (zB: keine Erdungsmöglichkeit, langflooriger Fußbodenbelag, …), so kann unter Umständen auch diese ekey net SE am gleichen RS 485 BUS die Abschaltung nicht mehr durfführen. Für diesen seltenen Fall gibt es eine **spezielle „ESD – Konfiguration“** mit zusätzlicher Hardware – **siehe Kapitel 14***

RFID Verwendung:



ekey net FS RFID können nach der grundsätzlichen Aktivierung der RFID Funktionalität in den Grundeinstellungen – Kapitel 8.1.1.2 individuell angepasst werden.

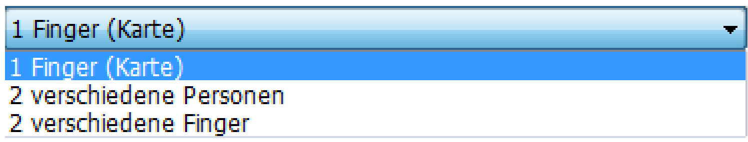


Die in den Grundeinstellungen definierte RFID Verwendungsart wirkt sich nur bei der Neuanlage von ekey net FS RFID aus. Individuelle Einstellungen an bestehenden Fingerscannern werden nicht aktualisiert.

Zutrittstype:

Zutrittstype | 1 Finger (Karte)

Der Parameter „**Zutrittstype**" definiert, wie der ekey net FS das Auslösen eines Ereignisses (z.B. mit Finger Türe öffnen) entscheidet. Dabei sind 3 Möglichkeiten vorgesehen.



- **1 Finger (Karte)** -> eine Person muss einen berechtigten Finger bzw. Karte zum Auslösen des Ereignisses über den Sensor ziehen. (Standardanwendung)
- **2 verschiedene Personen** -> 2 Personen müssen jeweils einen berechtigten Finger über den Sensor ziehen, damit der Fingerscanner das Ereignis auslöst (z.B. für Räume in denen immer 2 Personen anwesend sein müssen). Ausgelöst wird dabei das Ereignis des 1. gezogenen Fingers (also der ersten Person). Der Finger der 2. Person dient als Bestätigung.
- **2 verschiedene Finger** -> hier müssen 2 verschiedene Finger einer Person über den Sensor gezogen werden, damit das Ereignis ausgelöst wird.Ausgelöst wird dabei das Ereignis des 1. gezogenen Fingers. Der zweite Finger der Person dient als Bestätigung.

Max. Finger für L-Fingerscanner zulassen:

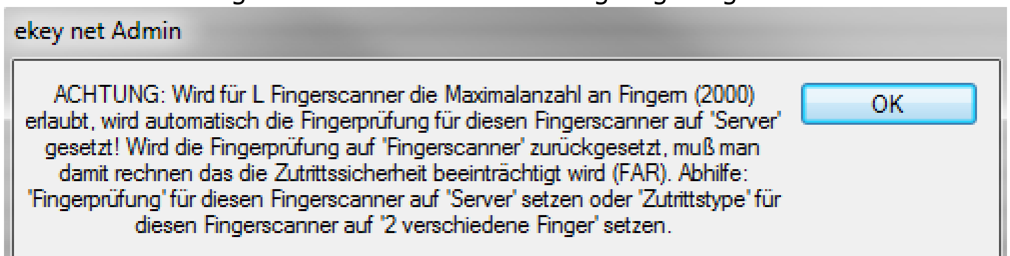
Max. Finger f. L FS zulassen ☐

ekey net FS des Typs „L" werden bei Installation standardmäßig nur mit einer Speicherkapazität von 200 Fingern installiert.

Max. Finger f. L FS zulassen ☑

Bei Aktivierung der maximalen Speicherkapazität von 2000 Fingertemplates erhöht sich, aufgrund der erhöhten Anzahl der durch zu führenden Vergleiche (Matches) der Fingertemplates, die theoretische Wahrscheinlichkeit für das Auftreten eines einzelnen FAR-Falles.

Es wird daher folgende Informationsmeldung angezeigt

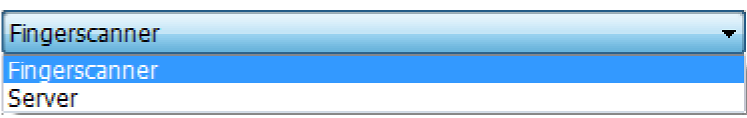


und die Fingerprüfung auf Servermatching umgestellt!

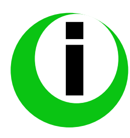
Fingerprüfung:

Fingerprüfung	Fingerscanner

Die Fingerprüfung (Matching = Template-Vergleich des gezogenen Fingers mit den Fingern in der Datenbank) wird grundsätzlich am Fingerscanner ausgeführt. Speziell bei einer großen Anzahl von Fingern (> 200) am ekey net FS,kann die Prüfprozedur lange (> 10Sekunden bis 50 Sekunden bei 2000 Fingern) dauern. Eine Möglichkeit die Prüfung in einer akzeptablen Zeit durchzuführen, ist Fingerprüfung „**Server**" zu definieren. Sind mehr als 200 Finger Speicherkapazität ausgewählt (möglich bei ekey net FS L), so wird automatisch „Server" eingestellt.



- Fingerscanner-> Fingerprüfung (Matching) wird am ekey net FS durchgeführt (für S und M Typen empfohlen)
- Server-> Prüfprozedur wird am ekey net Terminalserver durchgeführt (für L-Typen empfohlen)



Fingerprüfung „Server" funktioniert nur im Online-Betrieb. Ist der Fingerscanner offline (keine Verbindung zu ekey net Terminalserver), so wird die Fingerprüfung am Scanner durchgeführt. Die Entscheidung zum Zutritt kann damit erheblich länger dauern!

Zeitgesteuerte Wiedereintrittssperre (Min)

Wartezeit nach Zutritt (in Min)	0

Benutzer können nach einem Zutritt für einen Zeitraum gesperrt werden (Anti Pass Back), bis Sie wiederum Zutritt erlangen können (unabhängig vom Finger). Zieht ein Benutzer innerhalb dieser definierten Zeit (Wartezeit) den Finger über den Sensor, erhält der Benutzer eine Ablehnung. Die Wartezeit bezieht sich immer auf einen Benutzer und die Funktion gilt für alle zugewiesenen Benutzer am ekey net FS.

Die Zeit kann hier von

- 0… keine Sperre bis
- 60 … 60min

in Minutenschritten definiert werden.

Lageplan

Lageplan	

Hier können Sie einen Link zu einem Lageplan eingeben. (Externe Datei). Lagepläne können nicht von ekey net erstellt werden. Sie können den Link dann mit einem Doppelklick öffnen. Achten Sie dabei aber auf die Berechtigungen im Netzwerk (der Link muss vom Benutzer bzw. vom Rechner aus erreichbar sein)

Web-Aufzeichnung:

Web-Aufzeichnung	☐

Siehe Webaufzeichnung Kapitel 15.1.7



Nach einem Update von ekey net 3.x auf ekey net 4.x müssen Sie die Web-Aufzeichnung an den genwünschten ekey net FS aktivieren In den Vorgängerversionen wurde automatisch von allen ekey net FS aufgezeichnet.



Konto Web-Aufzeichnung:

Konto Web-Aufzeichnung	

Siehe Webaufzeichnung Kapitel 15.1.7

Benachrichtigungen:

Benachrichtigungen

Bei Zuständen oder Ereignissen, die am ekey net FS auftreten, können Nachrichten in folgenden Formen an definierte Empfänger abgesetzt werden:

Standard
- Standard
- kein E-Mail
- E-Mail an Administratoren
- E-Mail an Administratoren der Terminalgruppe

- Standard hier gilt die Einstellung, die im Bereich der Grundeinstellungen / Optionen für die Benachrichtigung gemacht wurde.Wählen Sie bei allen ekey net FS „Standard", so können Sie Änderungen der Benachrichtigungsfunktion zentral im Bereich „Optionen" durchführen. Sie dazu auch Kapitel 8.1.1
- kein E-Mail für diesen ekey net FS wird bei dem auftretenden Ereignis keine Benachrichtigung gesandt.
- E-Mail an Administratoren Bei dem auftretenden Ereignis wird ein E-mail an alle ekey net Administratoren des Systems gesandt.
- E-Mail an Administratoren der Terminalgruppe Bei dem auftretenden Ereignis wird nur ein E-mail an die für diesen Terminalserver berechtigten ekey net Administratoren gesandt.

Folgende Ereignisse können im Bereich des ekey net FS zuBenachrichtigungen führen:

Terminal offline	Standard
Terminal Kommunikationsprobleme	Standard
Terminal erster Schaltvorgang eines Tages	Standard
Terminal jeder Schaltvorgang	Standard
Terminal jeder Zutrittsversuch	Standard
E-Mail nach Fehlerbehebung	Standard
SMTP E-Mailserver	
Absender E-Mailadresse	
SMTP Anmeldeverfahren	Standard
SMTP Anmeldename	
SMTP Anmeldekennwort	

Für die Versendung der Benachrichtigungen sind Einstellungen abhängig von ihrer System- und Serverarchitektur vorzunehmen:

SMTP E-Mailserver	

Hostname oder Adresse des Postausgangs – Servers hier eintragen



Absender E-Mailadresse	

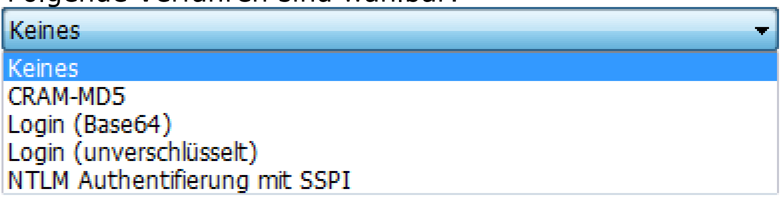
Die Emailadresse des Absenders, in diesem Fall von ekey net ist hier zu definieren (virtuelle Adresse).



Sie können an ekey net kein Email senden! Die hier eingegebene Adresse hilft ihnen, wenn Sie eine für sich sprechende Adresse wählen,in ihrem Posteingangsordner klar zu erkennen, von wem die Email kommt.

SMTP Anmeldeverfahren	Keines

Wählen Sie das korrekte Verschlüsselungsverfahren Ihres SMTP - Servers aus
Folgende Verfahren sind wählbar:





Die Einstellungen für die E-mailfunktionen, speziell im Hinblick auf den SMTP –Servers sind abhängig von ihrer Systemkonfiguration. ekey kann ihnen in diesem Bereich nureingeschränkt Unterstützung bieten. Wenn Sie diese Funktionen aktivieren möchten, ziehen Sie bitte ihre IT-Spezialisten für die Konfiguration zu Rate.

SMTP Anmeldename	

Wenn erforderlich - bei den meisten SMTP Servern kann dieses Feld leer bleiben

SMTP Anmeldekennwort	

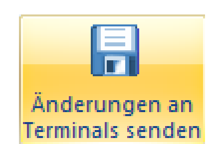
Wenn erforderlich - bei den meisten SMTP Servern kann dieses Feld leer bleiben



Bei Erstellung eines Fingerscanners über die Funktion **„Fingerscanner erstellen"**wird auch automatisch eine Steuereinheit mit dem Namen **„Neue Steuereinheit"** angelegt. Wenn Sie diese nicht benötigen, können Sie das Gerät jetzt löschen!

6.6.3.3 Änderungen an Terminals senden

Nach Abschluss aller Einstellungen klicken Sie auf den Button



bzw. führen Sie ein „Force Update" lt. Kapitel 6.5.1.2 durch!

Erst damit werden die Änderungen und Einstellungen im System aktiv!!



6.6.4 Bearbeiten von Terminals und Terminalgruppen

6.6.4.1 Änderung von Parametern

Terminalgruppen und Terminals können jederzeit bearbeitet werden und die entsprechenden Parameter überschrieben werden. Markieren Sie das gewünschte Objekt und starten Sie den ekey net Assistenten.



Änderungen der Objekte werden grundsätzlich immer mit dem Assistenten durchgeführt. Mit der Funktion **Objekt öffnen** wird dieser passend zum entsprechenden Objekt gestartet.

Objekt öffnen

6.6.4.2 Terminals und Terminalgruppen verschieben

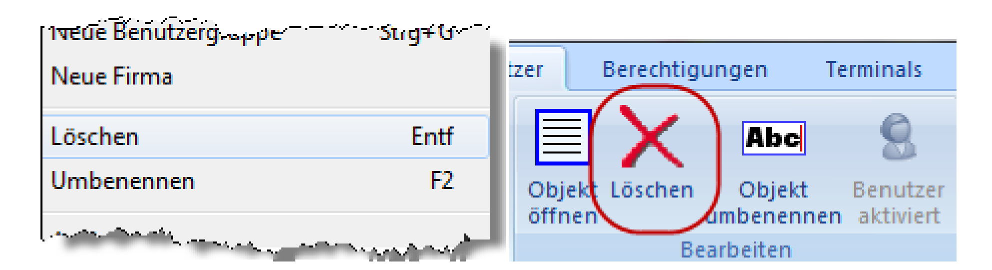
Mittels Drag&Drop können Sie im Terminalexplorer Terminals- und ganze Terminalgruppen verschieben. Achten Sie dabei aber auf die eventuell geänderten Berechtigungen!!

6.6.4.3 Force Update

Abschließend führen Sie Immer ein „**Force Update**" lt. Kapitel 6.5.1.2 durch.
Erst jetzt werden Änderungen im System aktiv !!

6.6.5 Löschen von Terminals und Terminalgruppen

KlickenSie mit der rechten Maustasteauf das zu löschende Terminal bzw. die Terminalgruppe. Es erscheint das Kontext-Menü:



Wählen Sie hier „**Löschen**" oder Klicken Sie in der Symbolleiste **„Bearbeiten" auf Löschen**

Bei der Löschung von Terminalgruppen, werden natürlich alle Terminals und Terminaluntergruppen der gewählten Terminalgruppe entfernt.

Abschließend führen Sie ein „**Force Update**" lt. Kapitel 6.5.1.2 durch.
Erst jetzt wird die Löschung im System aktiv !!

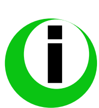
Wichtig ist hier anzumerken, dass die Terminals nicht sofort unwiederbringlich aus dem System gelöscht werden sondern im Terminalexplorer unter dem Bereich Gelöscht abgelegt werden. Sie können somit eine irrtümliche Löschung rückgängig machen, indem Sie die Terminal(gruppe) einfach wieder in die „aktive" Terminalgruppe" mit Drag&Drop zurückbefördern. Erst wenn Sie den Inhalt von Gelöscht leeren, sind die Daten unwiederbringlich verloren.

Filiale Wien
T_SRV Wien
Haupteingangstüren
Nebeneingangstüren
Gelöscht
Gel.aus Filiale Wien » T_SRV Wien » Nebeneingangstüren (09.03.2010 13:39:51)



6.6.6 Zeitfenster

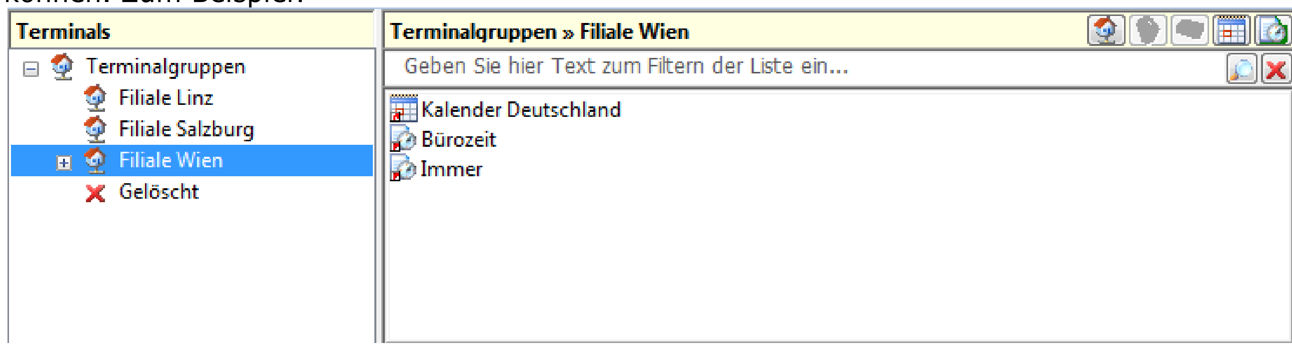
In den Zeitfenstern definieren Sie die zeitlichen Beschränkungen eines Zutritts von Personen und Personengruppen auf Tagesbasis über 7 Tage der Woche. Sie können die Zutrittszeiten dabei minutengenau definieren.



Grundsätzlich können Sie in jeder Terminalgruppen aber auch Terminalebene eigene Zeitfenster definieren. Es empfiehlt sich allerdings eher wenige Zeitfenster möglichst allgemeingültig zu verwenden, da die Übersichtlichkeit des Systems damit besser gewahrt bleibt.

Klicken Sie nun in das Terminalfenster und wählen Sie die gewünschte Terminalgruppe bzw. das Terminal.

Sie sehen nun im mittleren Fenster die Kalender und Zeitfenster, die in dieser Gruppe wirken können. Zum Beispiel:



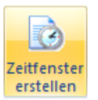
Hier haben Sie im Terminalgruppenbereich „Filiale Wien" die Zeitfenster

- Bürozeit
- Immer

zur Verfügung.

6.6.6.1 Neues Zeitfenster anlegen

Sie können nun

- durch ein Klick mit der rechten Maustaste in den Terminalgruppenbereichund Auswahl im Kontext- Menü „Neues Zeitfenster"
- oder durch Klick im Menü „Neu" auf den Button 

ein neues Zeitfenster anlegen.



Ein neues Zeitfenster wird immer in der gewählten Terminalgruppe angelegt und entsprechend der Definitionen in den Optionen (Kapitel 8.1.1) an die darunter liegenden Gruppen und Geräte vererbt.



Definieren Sie nun im Eigenschaften Fenster:

Eigenschaften | Zeiten | Zutrittsberechtigte

Eigenschaften - Zeitfenster	
Bezeichnung	Reinigung
Beschreibung	
Verbindungsfarbe	RGB (0, 0, 0)

Bezeichnung:

Bezeichnung	Reinigung

Bezeichnung des Fensters. Vergeben Sie hier einen sprechenden Namen für dieses Zeitfenster.

Beschreibung:

Beschreibung	

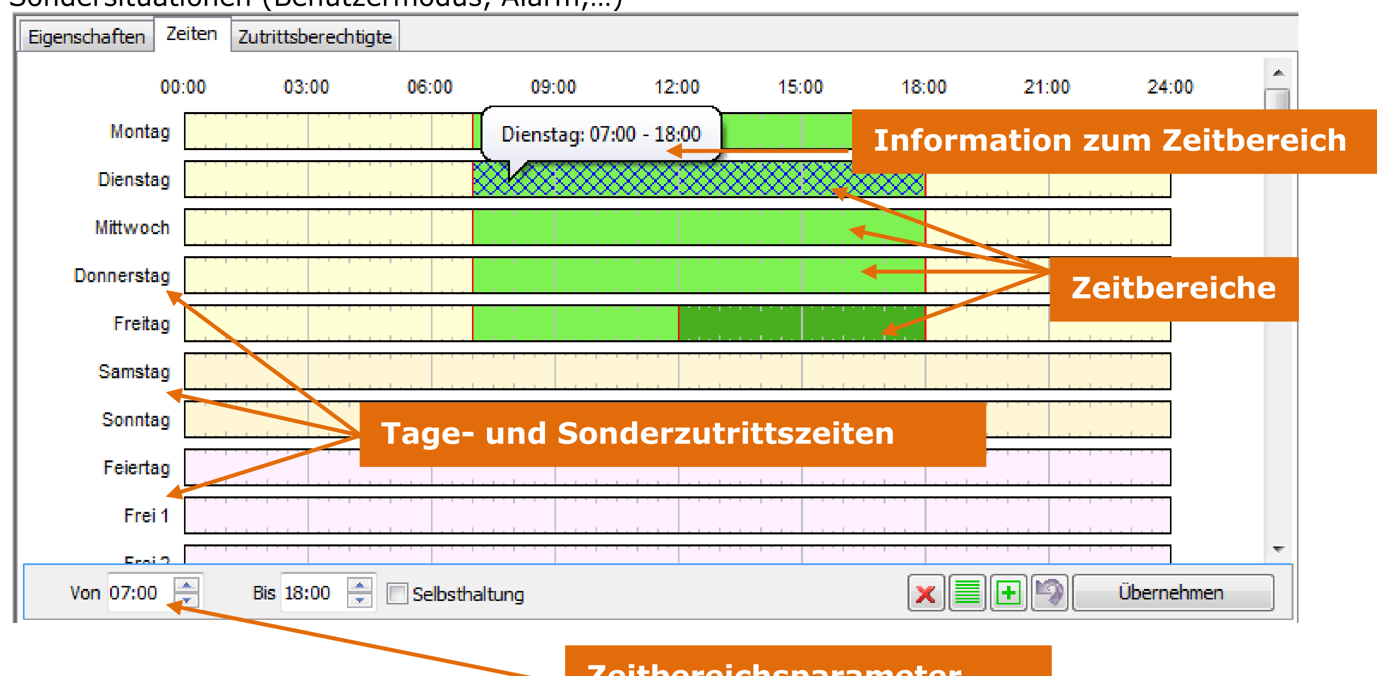
Hier können Sie eine freie Beschreibung eingeben, um weitere Informationen zu dem Zeitfenster zu erhalten.

Verbindungsfarbe:

Verbindungsfarbe	RGB (0, 0, 0)

Hier definieren Sie die Farbe, mit der dann die Verbindungslinien der Berechtigungen angezeigt werden (siehe auch Kapitel 6.5.1). Die Farbzuordnung der Linien hilft, bei komplexen Systemen die Übersichtlichkeit zu bewahren.

Im Reiter „**Zeiten**" definieren Sie nun die tatsächliche zeitliche Wirksamkeit dieses Fensters. Hier definieren Sie die einzelnen Zeitbereiche über die Wochentage, an denen Zutritt erlangt werden kann. Sie definieren Daueröffnungszeiten (Selbsthaltung) und Zutrittsrechte bei Sondersituationen (Benutzermodus, Alarm,…)



Um nun einen Zeitbereich für den Zutritt zu definieren klicken Sie mit der Maustaste in den Zeitbalken des gewünschten Tages oder den Sonderzeiten (Betriebsurlaub, Alarm,...) und halten Sie die Maustaste gedrückt. Sie können nun einen Balken bis zum Ende der gewünschten Zutrittszeit ziehen.
Die Farbe des Zeitbereichsbalkens sagt ihnen auch welche Art von Zeitbereich vorliegt:

... Zutritt

... Zutritt mit Selbsthaltung

... Zeitbereich ist zur Bearbeitung ausgewählt

Die Summe aller Zeitbereiche definiert die funktionalen zeitlichen Eigenschaften des Zeitfensters im ekey net !

Nach Abschluss aller Eingaben ist immer mit Klick auf den Button

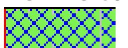
Übernehmen

die Übernahme der Eingaben zu bestätigen. Damit werden die geänderten Zeitbereichsdaten gespeichert. Damit Sie im System auch wirksam werden, müssenSie dann noch auf Klicken.

Änderungen an Terminals senden

6.6.6.1.1 Zeit von - bis

Definieren Sie hier die Uhrzeit, zu der ein Benutzer bzw. eine Benutzergruppe Zugang erhält. Die Zeiteinstellung ist auf die Minute genau möglich.
Wählen Sie mit einem rechten Mausklick den Zeitbalken, dessen Zeit Sie verändern möchten. Der Zeitbalken erscheint dann schraffiert.



Jetzt können Sie entweder die Zeitbereichsparameter des Balkens direkt als Wert eingeben,

Von 06:44 Bis 15:19

oder Sie verschieben Balkenanfang bzw. Balkenende mit der Maus (Klick und halten).
Klicken Sie in die Mitte des Balkens, so können Sie den ganzen Balken verschieben.

6.6.6.1.2 Selbsthaltung

STOP *Prüfen Sie unbedingt, ob ihr Schließsystem (Türöffner, Motorschloss, usw.) für eine Daueröffnung (Selbsthaltung) geeignet ist! Manche Schlösser können dies nicht, und eine dauernde Bestromung führt zum Defekt des Schließsystems!!*

Die Selbsthaltung ist eine spezielle Funktion im ekey net, die es erlaubt, eine Türe dauerhaft offen zu halten.



☐ Selbsthaltung oder ☑ Selbsthaltung

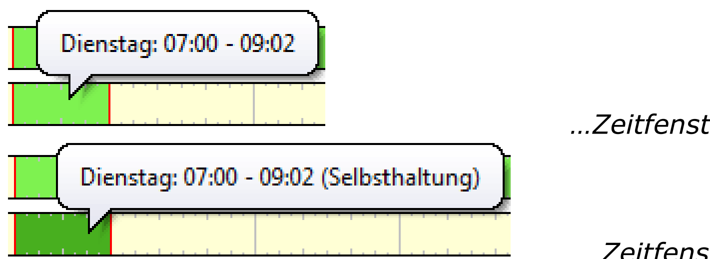
Wird die Selbsthaltung gewählt und ein berechtigter Finger über den Fingerscanner gezogen, so schaltet der zugehörige Anschluss dauerhaft bis

- zum Ablauf der Zeit (BIS-Zeit lt. 6.6.6.1)
- bis zum Auftreten der Aktion „**Anschluss X aus**“

ein.



Ob ein Zeiteintrag als Selbsthaltung definiert ist, sehen Sie an der Balkenfarbe und im Informationsfeld im Balken, wenn Sie mit dem Mauszeiger den Balken berühren.

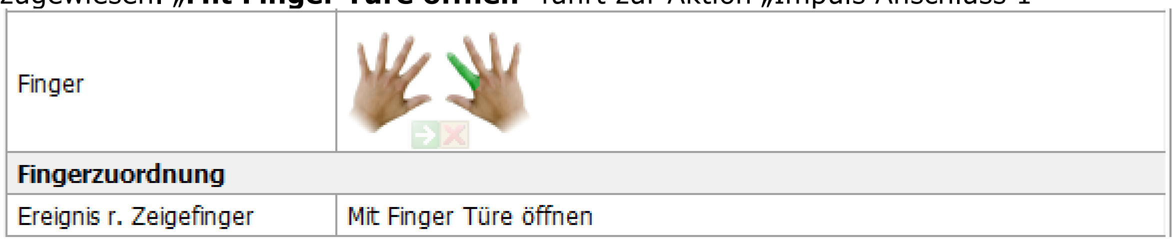


...Zeitfenster ohne Selbsthaltung

...Zeitfenster mit Selbsthaltung

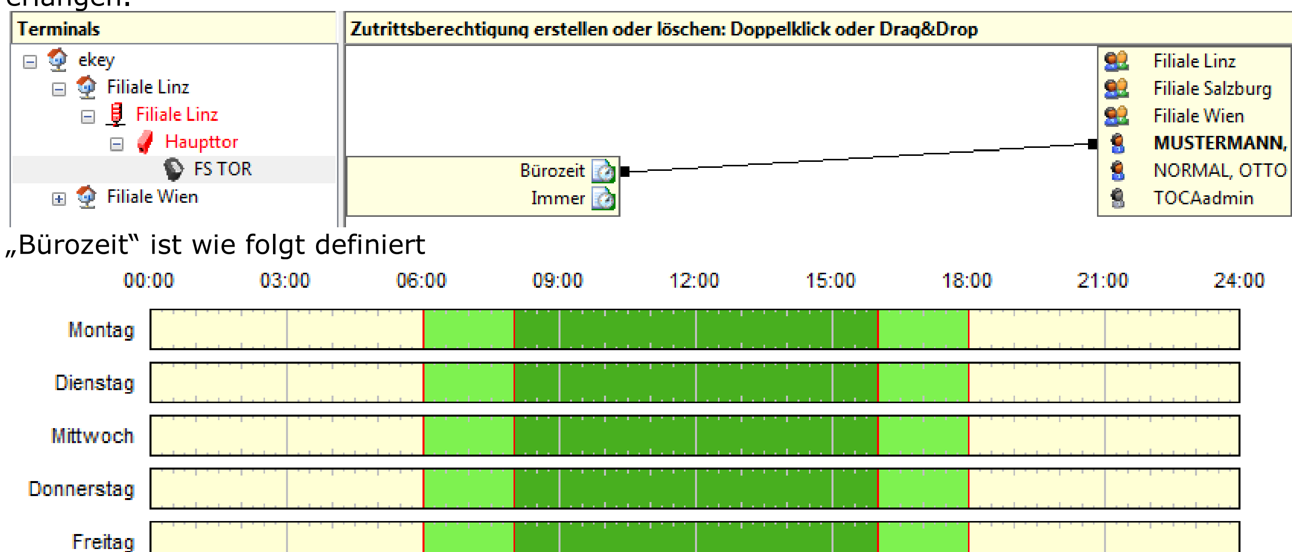
Beispiel

Max Mustermann hat am rechten Zeigefinger das Ereignis „**Mit Finger Türe öffnen**" zugewiesen. „**Mit Finger Türe öffnen**" führt zur Aktion „Impuls Anschluss 1"



Finger	
Fingerzuordnung	
Ereignis r. Zeigefinger	Mit Finger Türe öffnen

Hr.Mustermann ist berechtigt am Fingerscanner „FS TOR" in Linz zur „Bürozeit" Zutritt zu erlangen.



„Bürozeit" ist wie folgt definiert

Von Montag bis Freitag zwischen 06:00 und 08:00 Uhr kann er die Türe „FS TOR" öffnen (Impuls an Anschluss 1). In diesem Zeitraum geht die Tür aber nicht auf Daueröffnung. Zieht er den Finger nach 8 Uhr, so zieht das Relais (Anschluss1) dauerhaft an bis 16:00 Uhr. Dort fällt es dann selbsttätig ab. Von 16:00 bis 18:00 Uhr kann er die Tür wieder öffnen, ohne dass diese in Daueröffnen übergeht.

Von 18:00 bis nächsten Morgen um 06:00 Uhr, sowie Samstag und Sonntag ist für Hrn. Mustermann kein Zutritt möglich.





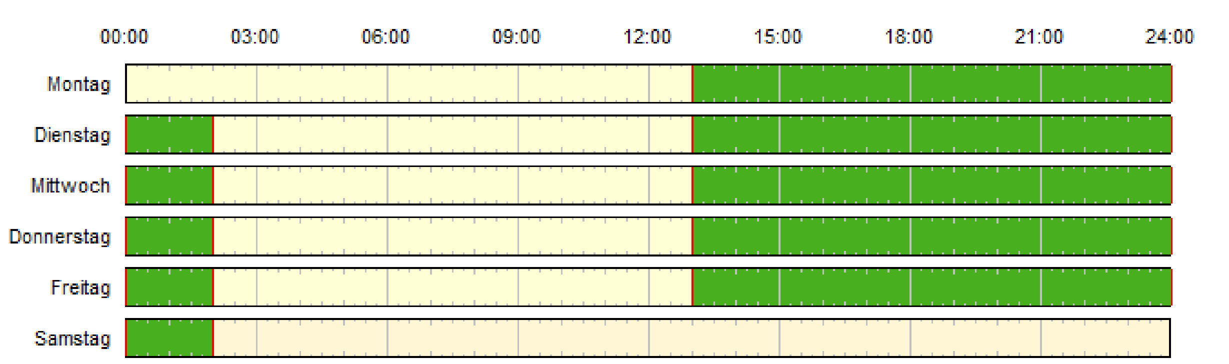
Das dauerhafte Einschalten des Anschlusses erfolgt immer durch einen berechtigten Finger. Eine reine Zeitsteuerung der Aktoren ohne vorherige Bestätigung durch einen berechtigten Finger ist nur mit der Funktion „Zeitsteuerung" möglich. So stellt man sicher, dass bei einer Daueröffnung bereits eine berechtigte Person anwesend ist.

Die Funktion findet sehr oft bei Geschäftstüren Anwendung, die tagsüber für die Kunden uneingeschränkt geöffnet sind. Außerhalb der Selbsthaltungszeit kann dann mit einem berechtigten Finger Zutritt erlangt werden, ohne dass die Tür dauerhaft geöffnet bleibt.

Selbsthaltung über Mitternacht.
Die Selbsthaltung wird generell immer mit dem definierten Ende des Zeitbereichs beendet und der Aktor (Anschluss) der zugewiesenen Steuereinheit fällt ab. Haben Sie beispielsweise eine Zeit
von 08:00 bis 12:00 definiert, so geht der zugewiesene Anschluss beim Ziehen eines Fingers nach 08:00 Uhr in Selbsthaltung und der Anschluss fällt um 12:00 Uhr selbsttätig ab.

Dies gilt natürlich auch analog, wenn Sie den Zeitbereich z.B. von 13:00 bis 24:00 definieren. **Hier gibt es aber eine Ausnahme**: Beginnt am nächsten Tag der Zeitbereich für die Selbsthaltung um 0:00 Uhr, so fällt das Relais nicht um 24:00, sondern mit dem Ende des zweiten Zeitbereichs, welcher um 0:00 beginnt, ab! So bleibt die Tür über Mitternacht hinweg geöffnet.

Beispiel:



In diesem Beispiel wäre die Selbsthaltung von Montag 13:00 Uhr beginnend jeweils bis zum nächsten Tag um 2:00 früh des Folgetages dauerhaft geöffnet. Samstag Abend gibt es keine Selbsthaltung.

Beachten Sie bitte, dass ein definierter durchegehender Zeitraum nur 1 x über Mitternacht laufen darf.
Nicht möglich ist: START am Montag 12:30 bis Mittwoch 2:00 ! Dies würde ein Abfallen des Relais am Dienstag 24:00 zur Folge haben.



Machen Sie eine Änderung bei den Zeitfenstern, unabhängig davon ob Sie dabei die Selbsthaltungszeiten verändern und aktivieren diese Änderungen durch„Änderungen an Terminals senden", so müssen Sie bei allen Türen, wo die Selbsthaltung aktiv ist, einmal einen berechtigten Finger ziehen, damit die Selbsthaltungszeiten übernommen werden!!! Tun Sie das nicht, fällt die Selbsthaltung zur Ende-Zeit nicht ab und die Tür bleibt unter Umständen offen!

6.6.6.1.3 Zeitsteuerung

Ab der ekey Version 4.0.6 ist es nun möglich, ein Zeitfenster zu erstellen, welches selbständig (ohne dass ein Benutzer einen Fingerscanner betätigt) ein Relais steuert.

Beispiel: Sie möchten täglich von 8-18 Uhr automatisch eine Türe dauerhaft öffnen.

Zuerst erstellen Sie bitte ein neues Zeitfenster wie unter Punkt 6.6.6.1 beschrieben.
In den Optionen markieren Sie dieses bitte als „ Zeitfenster zur Zeitsteuerung verwenden"

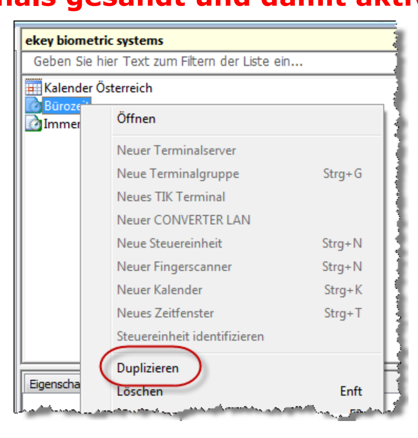
Dann wählen Sie die gewünschte Steuereinheit unter „Terminals" und weisen in den „Optionen" unter „Zeitsteuerung" dem gewünschten Relais Ihr neu erstelltes Zeitfenster zu.

6.6.6.1.4 Änderungen an Terminals senden

Klicken Sie nach Abschluss der Änderungen und Speicherung auf Änderungen an Terminals senden.
Erst jetzt werden die Eintragungen an die Terminals gesandt und damit aktiviert!

6.6.6.2 Zeitfenster duplizieren

Wenn Sie ein bereits angepasstes Zeitfenster in sehr ähnlicher Form noch einmal benötigen, so können Sie das Ausgangs-Zeitfenster sehr einfach duplizieren.
Klicken Sie mit der rechten Maus auf das Zeitfenster und wählen Sie aus dem Kontektmenü **„Duplizieren"**



6.6.6.3 Zeitfenster bearbeiten (ändern)

Zur Bearbeitung müssen Sie das gewünschte Zeitfenster mit einem Maus-Klick anwählen. Ändern Sie dann die Einstellungen analog wie in Kapitel 6.6.6.1 beschrieben.

Zeitbereiche löschen

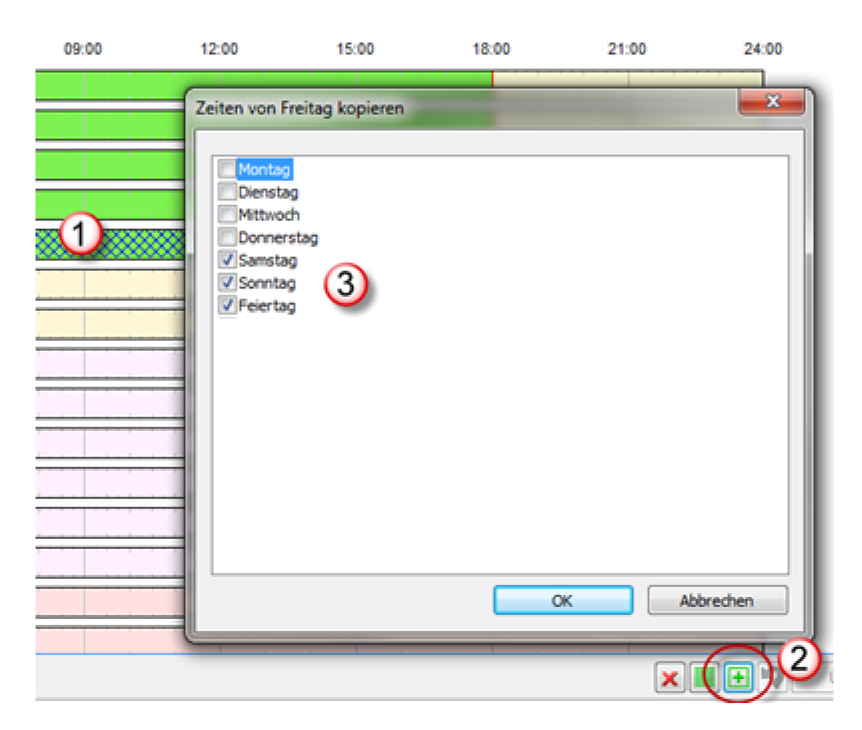
Um einen Zeitbereich zu löschen, wählen Sie den zu löschenden Balken mit einem rechten Mausklick. Er erscheint dann wiederum schraffiert .
Anschließend klicken Sierechts unten. Der gewählte Zeitbereich wird gelöscht.

Alle Tage Füllen

KlickenSie auf , so werden alle Tage und Sonderfunktionen mit einem Zeitbalken von 0-24Uhr ohne Selbsthaltung belegt. Es entsteht also ein Zeitfenster „Immer". Sie können dieses dann natürlich wieder entsprechend anpassen.

Tageszeiten auf weitere Tage kopieren

Um innerhalb eines Zeitfensters angepasste Tageszeiten auf weitere Tage zu kopieren, führen Sie folgende 3 Schritte durch und bestätigen den Vorgang mit OK.



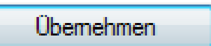
1. Wählen Sie bitte die zu kopierende Zeit durch eine Mausklick aus
2. Klicken Sie nun auf
3. Aktivieren Sie die gewünschten Zieltage und schließen Sie den Vorgang mit **OK** ab

Aktion rückgängig

Wenn Sie eine Aktion (Löschen, Verschieben eines Zeitbereichs,..) rückgängig machen wollen, klickenSie auf .Es können nur diejenigen Schritte zurückgenommen werden, die noch nicht gespeichert wurden (= Klick auf Button Übernehmen) revidiert werden.

Nach Abschluss aller Eingaben

ist immer mit Klick auf den Button

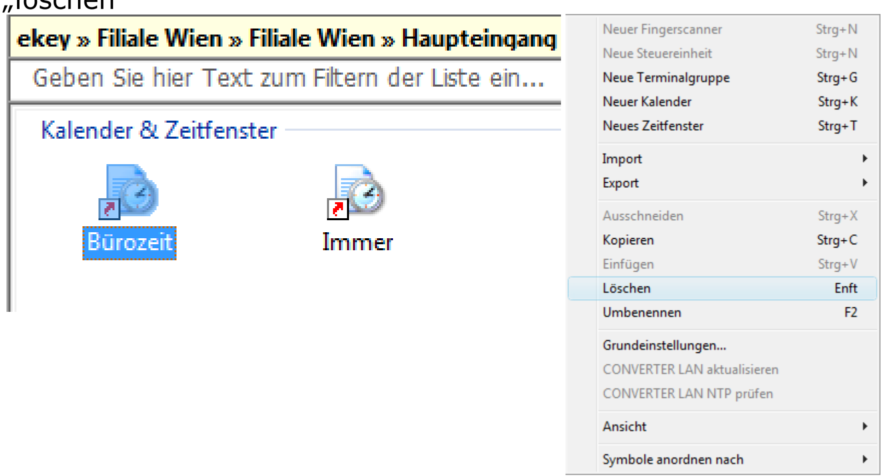


die Übernahme der Eingaben zu bestätigen. Damit werden die geänderten Zeitbereichsdaten gespeichert. Damit Sie im System auch wirksam werden, müssenSie dann noch auf„Änderungen an Terminals senden" Klicken.



6.6.6.4 Zeitfenster löschen

Durch einKlick mit der rechten Maustaste auf das Zeitfensterund Auswahl im Kontext- Menü „löschen"



wird das gewählte Zeitfenster gelöscht.



Ein Zeitfenster wird immer in der gewählten Terminalgruppe gelöscht. Entsprechend der Definitionen in den Optionen (Kapitel 8.1.1) an die darunterliegenden Gruppen und Geräte wird die Löschung vererbt. Ist in derübergeordneten Terminalgruppe das Fenster noch vorhanden bleibt es auch nach dem Löschen vorhanden.



Klicken Sie nach Abschluss der Löschung auf .
Erst jetzt wird die Löschung an die Terminals gesandt und damit funktional wirksam!

6.6.7 Kalender

Im Kalender definieren Sie nun die Feiertage und freien Tage (Betriebsurlaube usw.), an denen ein Zutritt in Abhängigkeit der Zeitfenster **nicht** gewährt werden darf.

Ausgenommen von der Zutrittsverweigerung auf Kalenderbasis sind:

- Zeitfenster „Immer"
- Explizite Ausnahme im Zeitfenster (Alarm 1-3, Benutzermodus 1-3)

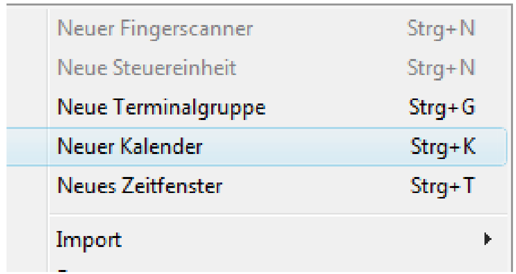
Grundsätzlich können Sie auf jeder Terminalgruppe aber auch Terminalebene einen oder mehrere Kalender definieren. Es empfiehlt sich nur einen (oder wenige) Kalender möglichst allgemeingültig zu verwenden, da die Übersichtlichkeit des Systems damit besser gewahrt bleibt. Legen Sie mehrere Kalender an, sind auch mehrere aktiv.

Die wirksamen Tage, an denen kein Zutritt möglich ist, sind damit die Summe aller Einträge in den Kalendern, die in der entsprechenden Terminalgruppe platziert sind.

6.6.7.1 Neuen Kalender anlegen

Einen neuen Kalender erstellen Sie

- Durch ein Klick mit der rechten Maustaste in die Terminalgruppenübersichtund Auswahl „**Neuer Kalender**“ im Kontext- Menü



- oder durch Klick auf den Buttonim Menü „Neu“.



Ein neuer Kalender wird immer in der gewählten Terminalgruppe angelegt und entsprechend der Definitionen in den Optionen (Kapitel 8.1.1) an die darunter liegenden Gruppen und Geräte vererbt.

Geben Sie nun folgende Daten im Eigenschaftenfenster des Kalenders ein.

Bezeichnung:

Bezeichnung	Sonderkalender Wien

Vergeben Sie hier einen sprechenden Namen für den Kalender. Speziell wenn Sie mehrere Kalender in ihrem System verwenden ist dies sehr hilfreich.

Beschreibung:

Beschreibung	

Freies Beschreibungsfeld für weitere Informationen zum Kalender.

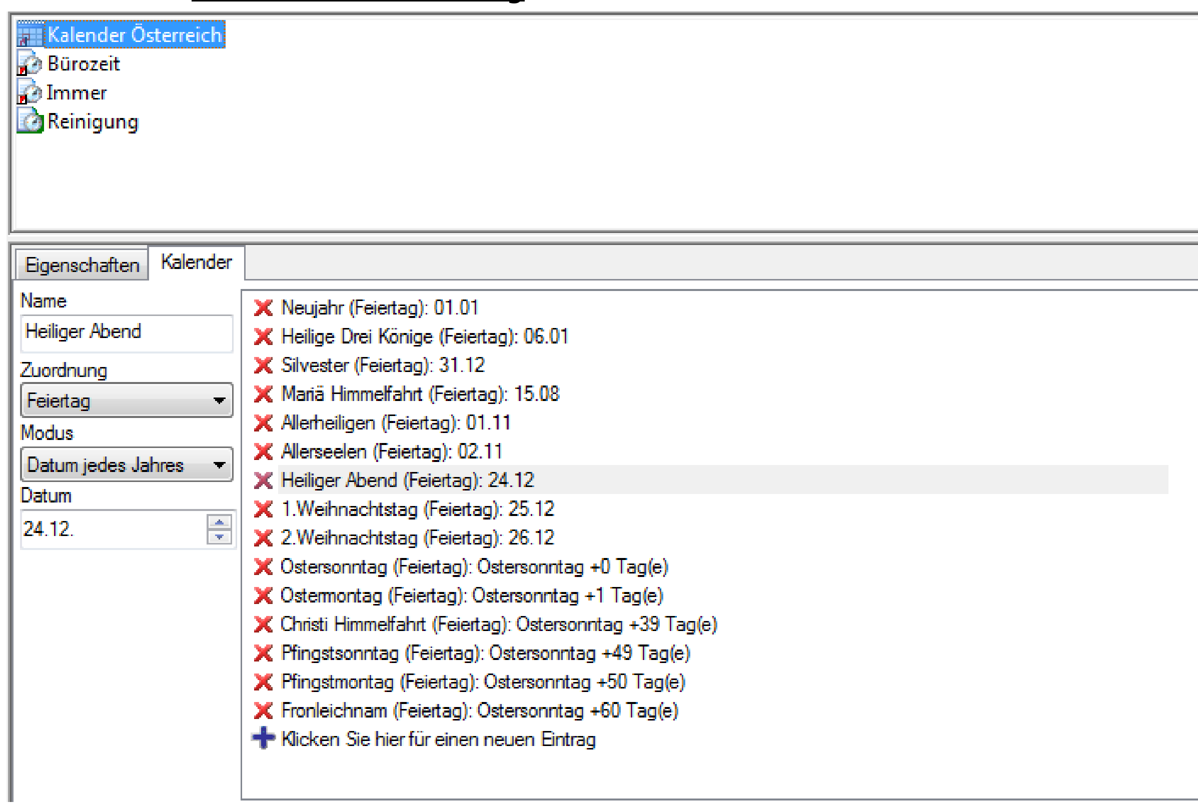
Im Reiter Kalender sehen Sie dann





6.6.7.2 Kalender erstellen

6.6.7.2.1 Neuer Kalendereintrag



Um einen neuen Kalendereintrag zu machen, klickenSie auf
Klicken Sie hier für einen neuen Eintrag
Um einen Kalendereintrag zu löschen klicken Sie auf das rote Kreuz
Silvester (Feiertag): 31.12 neben dem Eintrag



Es sind grundsätzlich ALLE für das entsprechende Land verfügbaren Feiertage vordefiniert. Wenn Sie zB nur die gesetzlichen Feiertage wünschen, müssen Sie alle anderen löschen!

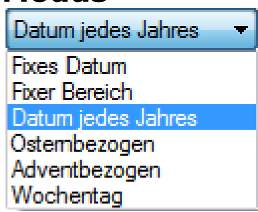
6.6.7.2.2 Parameter

Für jeden Kalendereintrag haben Sie die Parameter zu definieren

Name: Name des Feiertags, des freien Zeitraumes (z.B. Neujahr, Betriebsurlaub)



Modus

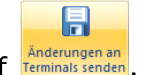


Hier definieren Sie nun die Eigenschaften des freien Tages / Feiertages im Jahresverlauf.

- **Fixes Datum**: ist ein Tag im definierten Jahr – der Tag wiederholt sich nicht jedes Jahr
- **Fixer Bereich**: ist z.B. Inventur findet immer vom 27 - 30. Juni statt.
- **Datum jedes Jahres**: ist ein fixes Datum jedes Jahr, z.B. Neujahr immer am 1.1.
- **Osternbezogen**: Der Feiertag bzw. Freie Tag hängt von Ostern ab, ekey net berechnet Ostern bis zum Jahr 2099. Definieren Sie einen Feiertag so, so stimmt er in jedem Jahr und Sie brauchen sich im das definitive Datum keine Gedanken machen. z.B. Pfingsten.
- **Adventbezogen**: Analogie zu osternbezogen
- **Wochentag**: ein Tag im Monat: z.B. jeder 1. Dienstag im Jänner.

Die Zeiteingabefelder ändern sich entsprechend des gewählten Modus.

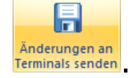
6.6.7.2.3 Änderungen an Terminals senden

Klicken Sie nach Abschluss der Parametrierungen auf .

Erst jetzt werden die Einstellungen an die Terminals gesandt und damit aktiviert!

6.6.7.3 Kalender Bearbeiten

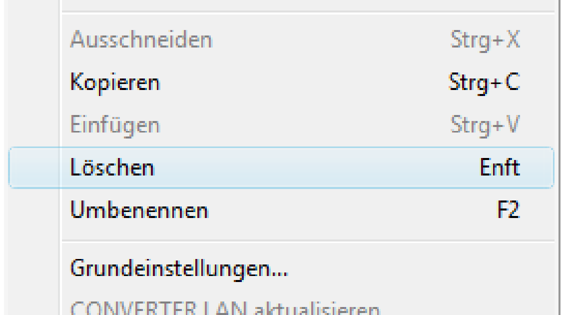
Zur Bearbeitung müssen Sie den gewünschten Kalender mit einem Maus-Klick anwählen. Ändern Sie dann die Einstellungen analog wie in Kapitel 6.6.7.2beschrieben.

Klicken Sie nach Abschluss der Änderung auf .

Erst jetzt werden die Änderungen an die Terminals gesandt und damit aktiviert!

6.6.7.4 Kalender löschen

Durch einen Klick mit der rechtenMaustaste in den Kalenderund Auswahl im Kontext- Menü „löschen"



wird der gewählte Kalender gelöscht.



Ein Kalender wird immer in der gewählten Terminalgruppe gelöscht. Entsprechend der Definitionen in den Optionen (Kapitel 8.1.1) wird die Löschung an die darunterliegenden Gruppen und Geräte vererbt. Ist in der übergeordneten Terminalgruppe der Kalender noch vorhanden, bleibt er es auch nach dem Löschen.

Klicken Sie nach Abschluss der Änderung auf Änderungen an Terminals senden.

Erst jetzt wird die Löschung an die Terminals gesandt und damit aktiviert!

6.7 Menü „STATUS“

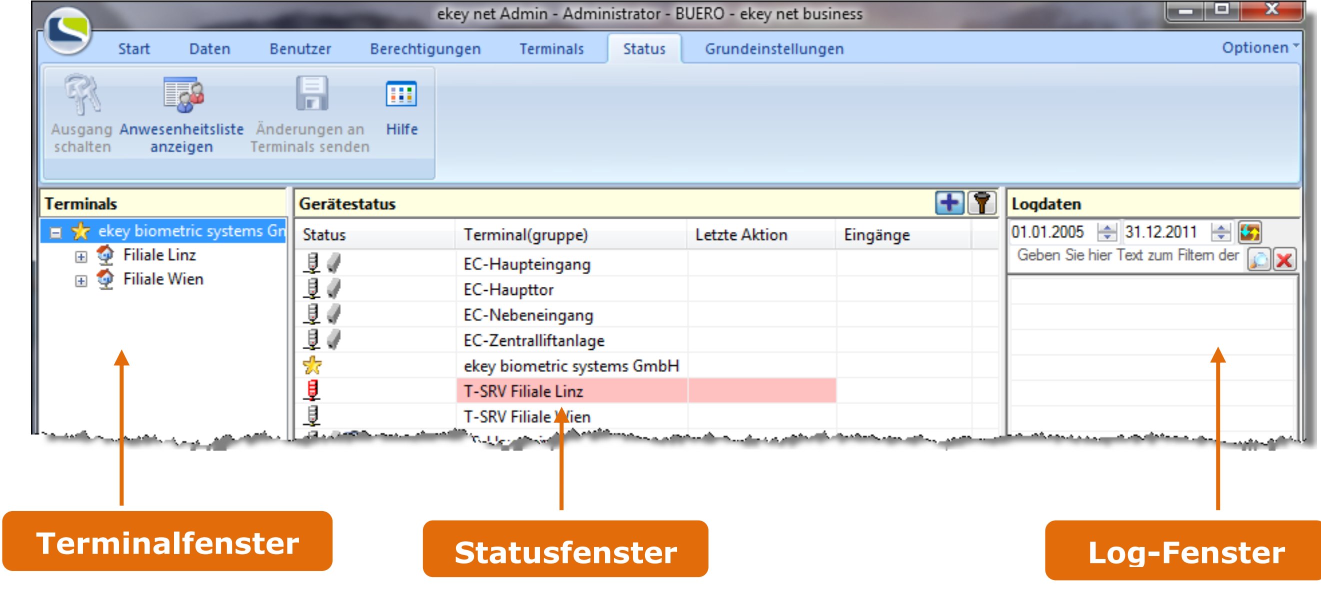
6.7.1 Allgemein

Der Gerätestatus im ekey net erlaubt ihnen die Prüfung des Zustandes der konfigurierten Geräte

- ekey net Terminalserver
- ekey net CV LAN
- ekey net FS
- ekey net SE

im System ekey net

Nach dem Start des ekey net Admin klicken Sie auf dieMenügruppe „**Status**“



Die Ansicht zeigt die

- Terminalstruktur,
- Statusfenster (Status der Geräte in der gewählten Terminalgruppe) und
- Log-Fenster (Logeinträge zu einem gewählten Gerät)

Im Statusfenster werden immer die Geräte der im Terminalfenster gewählten Terminalgruppe angezeigt.



6.7.2 Das Statusfenster

Im Statusfenster sieht man nun der Zustand der Geräte der im Terminalfenster gewählten Terminalgruppe. Über die Auswahl im Terminalfenster kann man so die Ansicht übersichtlicher gestalten.

Gerätestatus

Status	Terminal(gruppe)	Letzte Aktion	Version bei letzter Aktualisierung	Benutzer bei letzter Aktualisierung	Finger bei letzter Aktualisierung
	TESTUSERPC		4.0.4.9		
	134				
	138				
	70				
	Terminalgruppen				
	TEST3-PC		4.0.4.12		
	54				
	FS_134	08:34:30	5.3.3.1	0	0 (200 frei)
	FS_138	14:54:24 15.04.2010	5.3.3.1	0	0 (40 frei)
	FS_54		5.3.3.1	0	0 (200 frei)
	FS_70	14:54:00 15.04.2010	5.3.3.1	0	0 (2000 frei)
	SE_134		0.0.0.0		
	SE_138		1.34.3.31		
	SE_54		1.34.3.31		
	SE_70		1.34.3.31		

Finger bei letzter Aktualisierung: Zeigt die Fingeranzahl am Terminal (Fingerscanner). Bei der Anzeige:

- 0(Maximum Fingerscanner)… ist die Fingeranzahl unbekannt.
- z.B. 20 von 2000 bedeutet das 20 Finger von maximal 2000 (L-Fingerscanner) am Fingerscanner geladen sind.

Benutzer bei letzter Aktualisierung: zeigt die Anzahl der Benutzer die am Fingerscanner geladen wurden.

Firmwareversion des Gerätes: 0.0.0.0 = Version ist nicht bekannt

Letzte Aktion: Zeitpunkt der letzen Aktion am Gerät

Terminal(Gruppe): Bezeichnung (Name) der Terminalgruppe bzw. des Terminals.

Anschlüsse: (nur bei ekey net SE und ekey net FS REL):
Zeigen den Zustand der Anschlüsse Relais 1,2 und 3 (von links nach rechts).
Gelb… Zustand unbekannt
Grün… Relais geschalten
Grau… Relais nicht geschalten

Geräte: Farbdarstellung zeigt, ob Gerät ONLINE oder OFFLINE ist:
Rot …. Offline
Grau… Online
Gelb… Aktion am Gerät notwendig (z.B. Tastendruck am Gerät notwendig – „Reset einer ekey net SE")

Bei der ekey net SEIN und der ekey net SEmini sind auch digitale Eingänge verfügbar die z.B. für Türzustandsüberwachungen verwendet werden können. Um den Zustand dieser Eingänge zu sehen muss die Ansicht im Statusfenster gewechselt werden. Klicken Sie dazu auf das Symbol ⊞ in der rechten oberen Ecke des Statusfensters.
Die Ansicht des Statusfensters wechselt auf folgende:

Gerätestatus

Status	Terminal(gruppe)	Letzte Aktion	Eingänge
	Haupteingangstüren		
	Haupteingang		
	Haupteingang Nord		
	Haupteingang Ost	10:08:37 29.05.2009	
	Haupteingang Süd		
	Haupteingang West		

Eingänge:
Hier ist nun der Zustand der Eingänge dargestellt:

- Gelb… Zustand ist unbekannt
- Grün.. Eingang ist geschlossen (Kurzschluss an Eingangspins)
- Grau… Eingang ist offen .

Die Eingänge der ekey net SE miniwerden im ekey net hauptsächlich für die Türzustandskontrolle verwendet.

6.7.3 Logging im Gerätestatus

Siehe dazu Kapitel 6.3.1

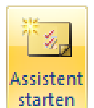
6.8 Menü „Grundeinstellungen“

Siehe dazu Kapitel 8

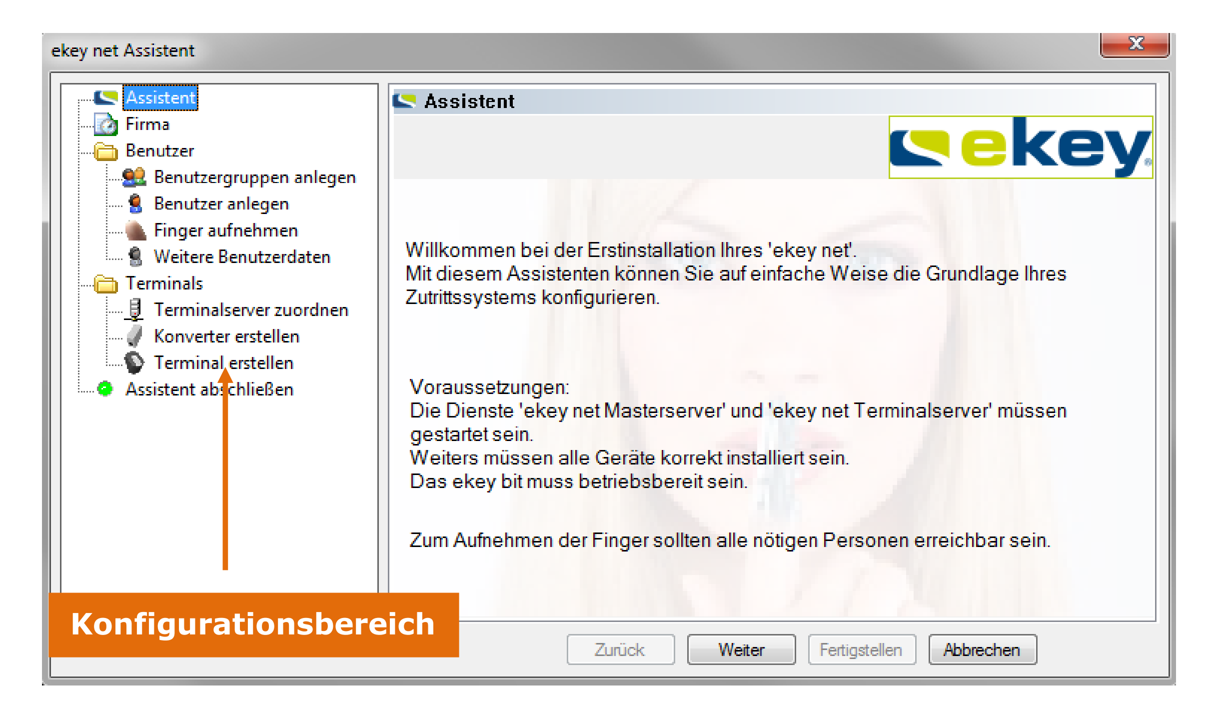


7 Der Assistent

Mit dem Assistenten können Sie auf einfache und unkomplizierte Weise ihr System ekey net schrittweise konfigurieren.



Der Assistent startet automatisch beim erstmaligen Aufruf von ekey net Admin bzw. wenn noch keine Eingaben (Konfigurationen) gemacht wurden. Sie können ihn aber auch im Menü „**Start**" jederzeit mit einem Klick starten.



Sie können nun durch Klick auf den Buttonmit der Konfiguration beginnen, oder Sie wählen im Konfigurationsbereich die Teile aus die Sie der Reihe nach konfigurieren möchten.

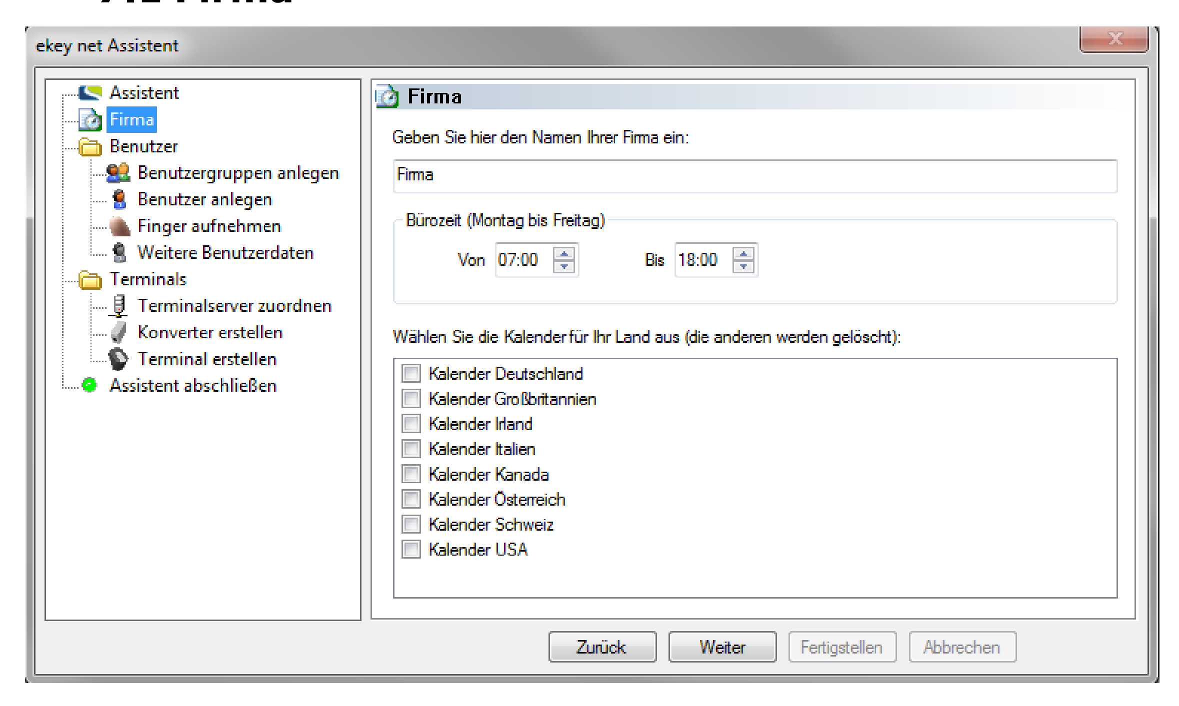
Die Hinweise zu den notwendigen Einträgen sind im Programm selbst weitgehend selbstsprechend und werden nicht mehr näher beschrieben. Die Wirkungsweise der einzugebenden Parameter ist hier nicht beschrieben und sollte in den entsprechenden Kapiteln nachgelesen werden.

Die Konfigurationsbereiche des Assistenten werden nun der Reihe nach gelistet und Sie sehen dazu die entsprechenden Verweise zu den relevanten Kapiteln dieses Handbuches.

Um den Assistenten abbrechen zu können muß im System mindestens 1 Kalender definiert worden sein.

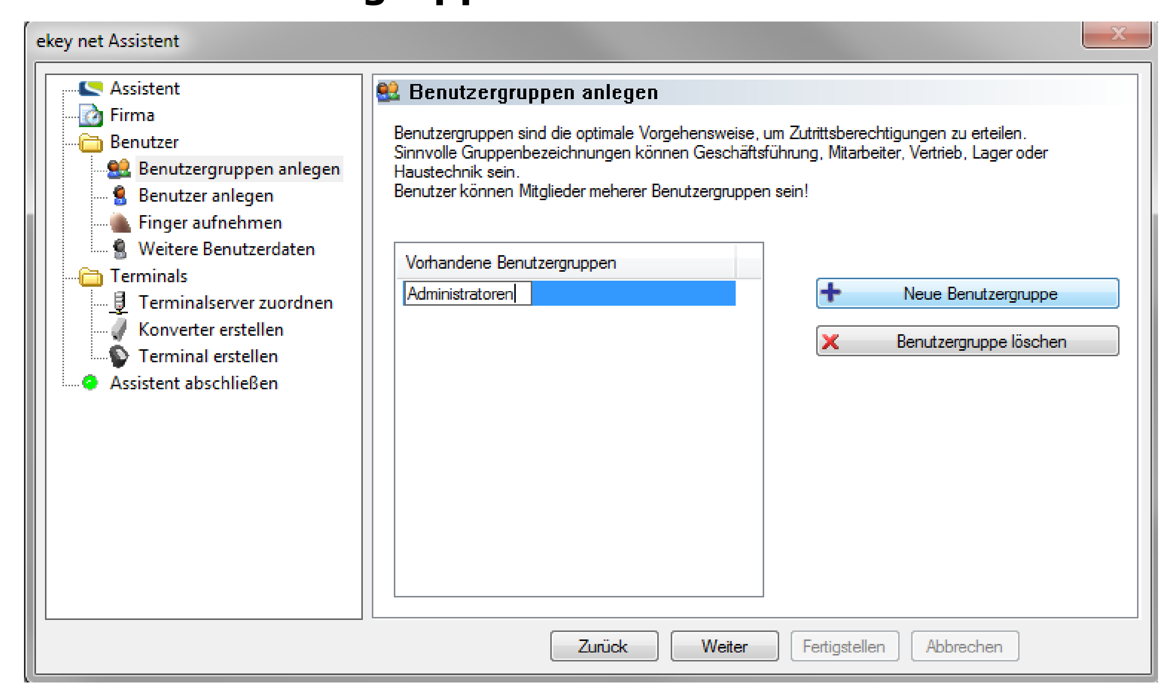


7.1 Firma



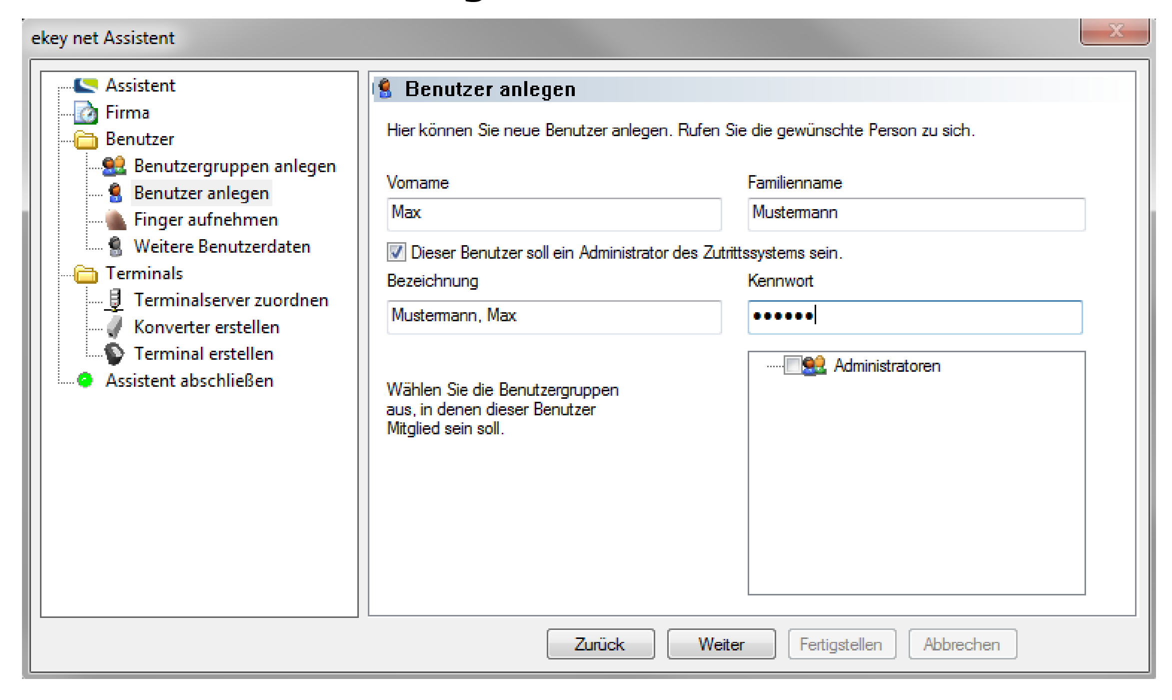
Hier geben Sie den**Namen** ihrer Firma / Organisation an, das Zeitfenster **Bürozeit**kann definiert werden (allerdings nur beim ersten Start des Assistenten) und der/die **Kalender**.

7.2 Benutzergruppen



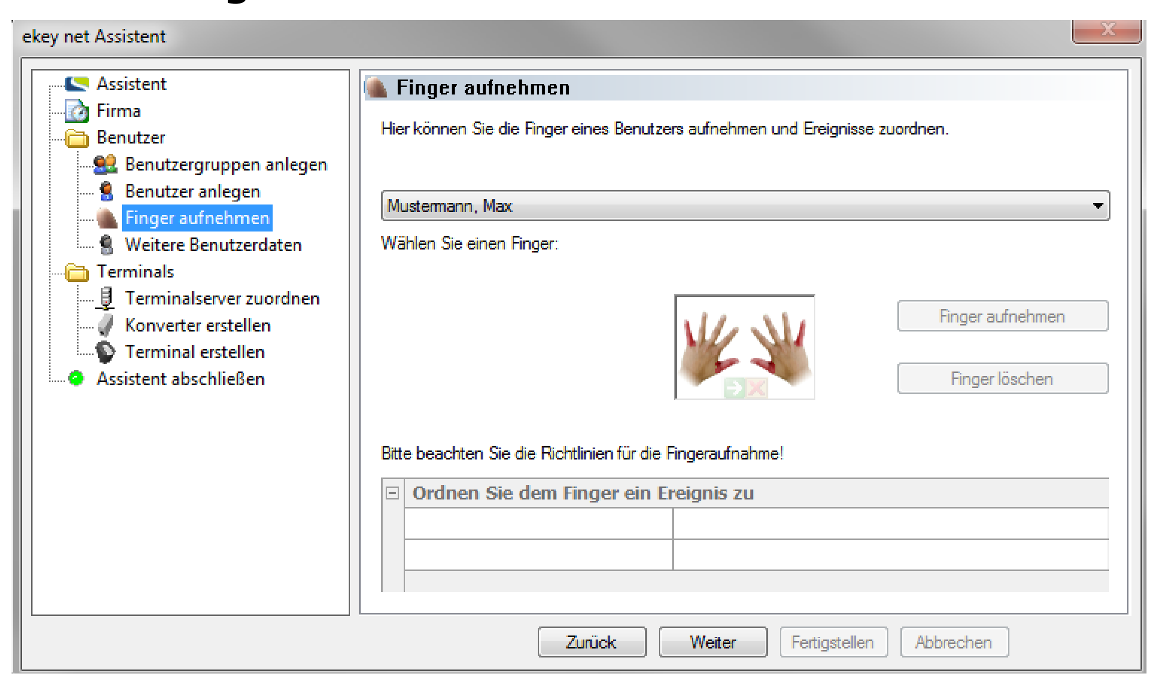
Hier können Sie **Benutzergruppen** anlegen und löschen. Siehe dazu Kapitel6.4.2.1

7.3 Benutzer anlegen



Anlage der **Benutzer** (Kapitel 6.4.2.2)und Zuordnung zur **Benutzergruppe**.

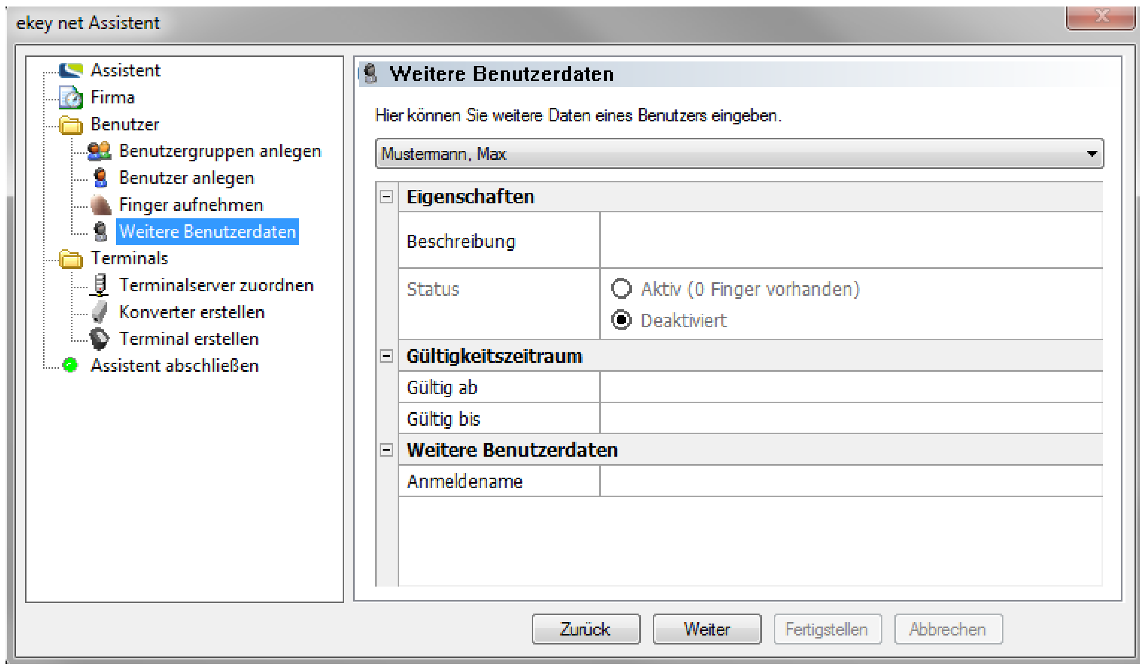
7.4 Fingeraufnahme



Hier können Sie für die angelegten **Benutzer** die einzelnen **Finger** aufnehmen und jedem Finger ein **Ereignis** zuordnen. (Kapitel 6.4.2.2)

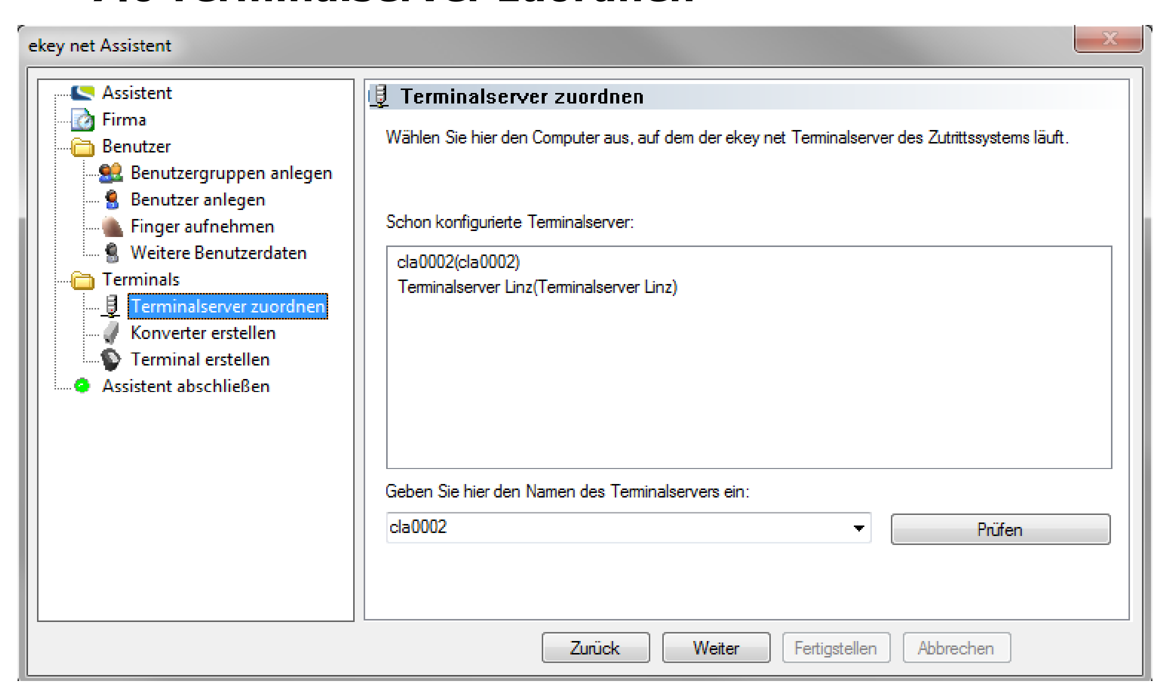


7.5 Weitere Benutzerdaten



Die Erfassung weiterer Benutzerdaten ist im Kapitel 6.4.2.2 näher beschrieben

7.6 Terminalserver zuordnen



STOP Bevor Sie hier weiter fortfahren, sollten Sie unbedingt das Kapitel 6.5 lesen. Sie finden dort einige Hinweise zur Planung, Installation und Systemarchitektur.

STOP **Ist keine Freie Lizenz mehr verfügbar, so ist eine Geräteanlage im ekey net mit dem Assistenten NICHT mehr möglich! Legen Sie zusätzliche ekey net SE dann lt. Kapitel 6.6.3.2.1an.**

Hier konfigurieren Sie ekey net Terminalserver (Kapitel 6.6.3.1.2).



ekey net Terminalserver (bzw. der PC/Server auf dem der ekey net Terminalserver installiert ist) muss über seinen NAMEN (DNS) im Netzwerk erreichbar sein. Prüfen Sie dies vorab! Haben Sie hier Schwierigkeiten nehmen Sie Kontakt mit einem Netzwerkspezialisten auf.

Nachdem Sie den Namen des ekey net Terminalservers eingegeben haben, können Sie mit dem Buttonprüfen, ob dieser tatsächlich vom ekey net Masterserver aus erreichbar ist.

Der Assistent meldet dann z.B:

Der Computer ekeynet konnte vom Masterserver aus erreicht werden. -> OK

Der Computer heidi konnte vom Masterserver aus nicht erreicht werden. -> NOK

Falls keine Verbindung herstellbar ist, prüfen Sie:

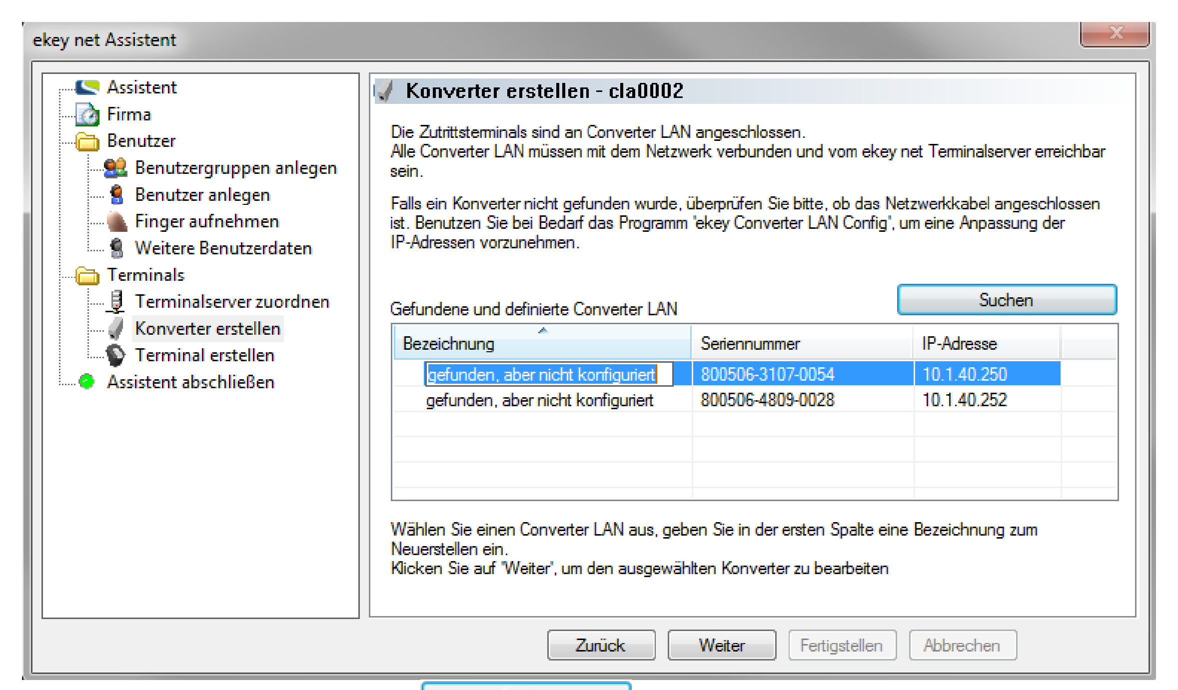
- Netzwerkeinstellungen (Namensauflösung)
- Ist der Dienst (ekey net Terminalserver)korrekt am gewählten ekey net Terminalserver installiert und aktiv !

Haben Sie mehrere ekey net Terminalserver konfiguriert, so müssen Sie nun einen wählen um die ekey net CV LAN zu konfigurieren. Sie müssen jetzt für jeden einzelnen ekey net Terminalserver die ekey net CV LAN abhängig von Ihrer Systemarchitektur konfigurieren (Kapitel 6.6.1)

7.7 Konverter erstellen



Bevor Sie hier weiter fortfahren, sollten Sie unbedingt das Kapitel5.2.3 durcharbeiten und die ekey net CV LAN entsprechend mit dem ekey net CV LAN config - Tool parametrieren.



Mit Klick auf den Button Suchen werden alle über den gewählten ekey net Terminalserver erreichbaren ekey net CV LAN gelistet.



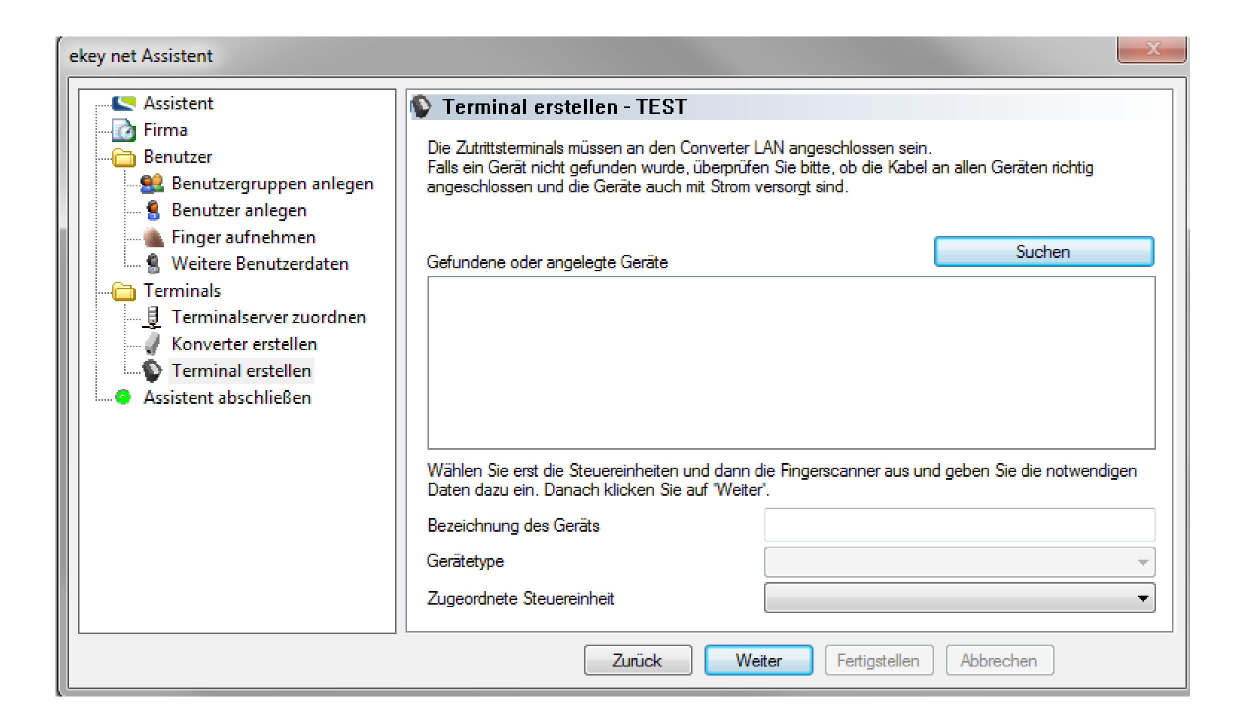
Geben Sie den einzelnen ekey net CV LAN nun eine „**Bezeichnung**" indem Sieden entsprechenden Converter mit einem Klick wählen und dann einen weiteren Klick in das Bezeichnungsfeld auf diesen machen.

Nun wählen Sie einen ekey net CV LAN und klickenauf Weiter .Klicken Sie auf die Tabellenfelder „Bezeichnung", „Seriennummer" oder „IP-Adresse", so werden die einzelnen entsprechend der Bedingung sortiert.

Ist ein ekey net CV LAN nicht in der Liste auffindbar so:

- Versuchen Sie die Suche zu wiederholen
- Prüfen Sie die Netzwerkverbindungen (LAN). Ist der ekey net CV LANpingbar?(Kapitel 5.2.3.4.1)
- Prüfen Sie die Spannungsversorgung des ekey net CV LAN

7.8 Terminal erstellen



Klicken Sie auf den Button Suchen . Das System sucht nun alle Geräte (ekey net FS und ekey net SE), die an den gewählten ekey net CV LAN angebunden sind und listet diese unter „**gefundene oder angelegte Geräte**".

Wählen Sie dann die Geräte der Reihe nach aus und geben Sie jedem einzelnen eine sprechende Bezeichnung, definieren Sie den Gerätetyp (wird normalerweise bereits von ekey net erkannt und automatisch eingetragen) und weisen Sie dem ekey net FS eine Steuereinheit zu, die als Schalt-Aktor für den Fingerscanner wirkt. Siehe auch Kapitel 6.6.3.2.



Finden Sie ein Gerät nicht in der Liste, so:

- Versuchen Sie die Suche zu wiederholen
- Prüfen Sie die Bus-Verbindungen (RS485) zum ekey net CV LAN.
  - Polung
  - Leitungsunterbrechung
  - Leitungslänge und Abschlusswiderstand
- Prüfen Sie die Spannungsversorgung der ekey net Geräte

Wiederholen Sie das nun für alle Geräte, indem Sie zu Abschnitt 7.7 durch Auswahl im Konfigurationsbereich zurückgehen und den nächsten ekey net CV LAN wählen, bzw., wenn dort alle ekey net CV LAN abgearbeitet sind, für den nächsten ekey net Terminalserver lt. Abschnitt 7.6.

8 Grundeinstellungen und Systemanpassungen

Im ekey net Admin können Sie neben den Berechtigungen und Geräteanlagen zum Betrieb auch eine Vielzahl von Parametern definieren. Sie können

- neue Ereignisse
- neue Aktionen
- neue Gerätetypen
- neue Benutzereigenschaften
- uvm.

kundenspezifisch definieren. Somit können Sie Ihr System an Ihre Anwendung perfekt anpassen. In den folgenden Kapiteln sehen Sie diese Möglichkeiten der Systemanpassung beschrieben.

8.1 Grundeinstellungen

Die Einstellungsmöglichkeiten sind analog zu den Funktionseinschränkungen – Kapitel 3.3 angepasst:



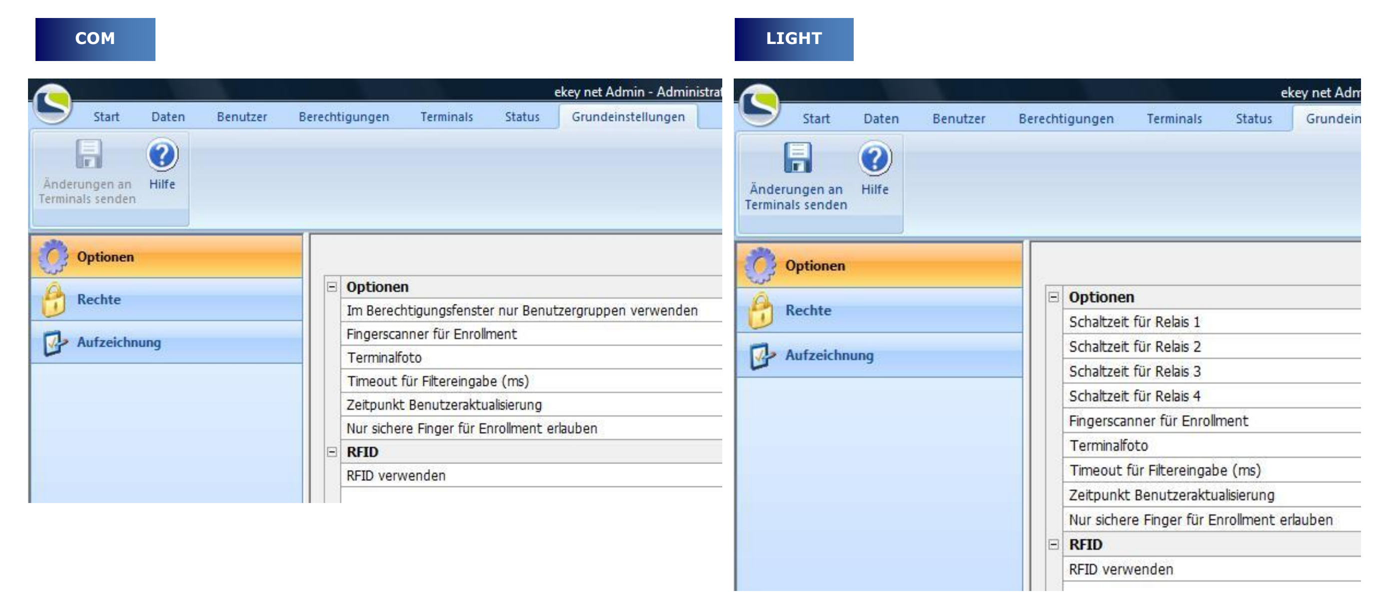
© 2010 – ekey biometric systems GmbH



8.1.1 OPTIONEN

8.1.1.1 OPTIONEN







Im Berechtigungsfenster nur Benutzergruppen verwenden:

Im Berechtigungsfenster nur Benutzergruppen verwenden	☐ Nein

Werden sehr viele Benutzer verwaltet, so wird die Übersicht im Berechtigungsfenster durch Aktivierung dieser Funktion verbessert.

COM BUSINESS



Einzelbenutzer werden dann im Benutzerexplorer nicht mehr angezeigt!

Wiegand ID verwenden:

Wiegand-ID verwenden	☐ Nein

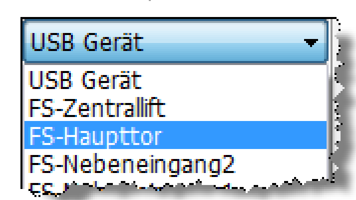
Das Feld „Wiegand-ID" wird in den Benutzer- und Terminaleigenschaften zur Verfügung gestellt.

BUSINESS

Fingerscanner für Enrollment:

Fingerscanner für Enrollment	USB Gerät

Zur Erfassung der Fingertemplates kann entweder das „USB Gerät" ekey bit oder ein beliebiger ekey net FS verwendet werden.

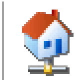


Die endgültige Auswahl des ekey net FS kann dann noch bei der Fingeraufnahme geändert werden.

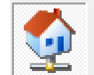


Unabhängig von dieser Einstellung wird bei einer Remotedesktopverbindung auf den Masterserver immer das USB Gerät deaktiviert, da in der Praxis der Server dann meistens nicht physisch zugänglich ist und daher kein USB Erfassungsgerät vorhanden sein wird.

Standardsymbol für Terminalgruppen:

Standardsymbol für Terminalgruppen 

Wird ein neues Terminal angelegt, so wird dieses Symbol als "Standard" zugeordnet. Sie können das Symbol dann natürlich für jedes einzelne Terminal als Eigenschaft ändern.
Folgende Symbole stehen zur Verfügung:

BUSINESS

Timeout für Filtereingabe

Timeout für Filtereingabe (ms)	1500

Wenn Sie einen Suchbegriff in ein Filterfeld schreiben (z.B.: Benutzersuche, Statusanzeige, ..), so wird nach dem letzten Tastendruck der hier definierte Wert in Millisekunden gesucht, und anschließend die Suche abgebrochen.

LIGHT COM BUSINESS

Zeitpunkt Benutzeraktualisierung:

Zeitpunkt Benutzeraktualisierung	01:30



Das System überträgt die erlernten Fingertemplates aus der Funktion des sog. "**Lernfingers**" zum angegebenen Zeitpunkt an die Fingerscanner (1 x täglich). Der Zeitpunkt sollte so gewählt werden, dass zu diesem wenige bis keine Benutzer das System bedienen, da es während der Datenübertragung zu verlangsamter Erkennung kommen kann.

LIGHT COM BUSINESS

Nur sichere Finger für Enrollment erlauben:

Nur sichere Finger für Enrollment erlauben	☑

Zur Vermeidung von angeblichen FAR (FalschAkzeptanzRate) – Fällen durch berechtigte Fingertemplates, die sich extrem ähnlich sind, wird die Aufnahme von Daumen und Kleinerfinger standardmäßig verhindert. Daumen und Kleinerfinger haben sehr wenige Minutien und damit sehr viel Fingerfläche, welche nicht eindeutig differenziert werden kann.

LIGHT COM BUSINESS

8.1.1.2 RFID

RFID verwenden:

RFID verwenden	☑ Ja

Werden in Ihrem ekey net FS mit der Funktion RFID verwendet, so ist diese Einstellung zu aktivieren. Sie können ansonsten nichts im ekey net für RFID konfigurieren.

LIGHT COM BUSINESS

Desktop-RFID-Leser:

Desktop-RFID-Leser	nicht verwenden oder nicht vorhanden

Hier definieren Sie die Verwendung des USB-RFID-Scanners zum Einlesen der RFID-Karten-Id's ins System ekey net.

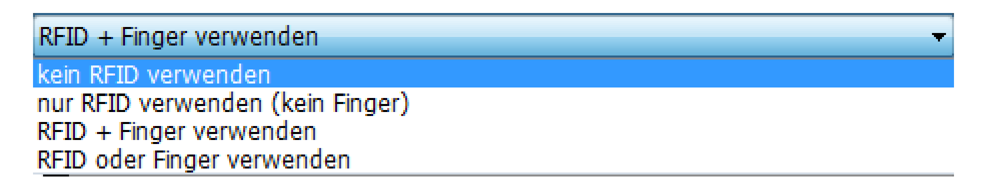
nicht verwenden oder nicht vorhanden
nicht verwenden oder nicht vorhanden
TRH-SR-100

Nicht verwenden oder nicht vorhanden: Sie können hier dann die Karten ID's auch über die im System vorhandenen ekey net FS RFID einlesen.
TRH-SR-100: Von ekey freigegebenes Gerät zur Erfassung der Karten IDs.

Standardvorgabe „RFID Verwendung"

Standardvorgabe 'RFID Verwendung'	RFID + Finger verwenden

Hier definieren Sie die Standardvorgabe beim Anlegen eines neuen Terminals. Sie können natürlich bei jedem einzelnen neuen Terminal die Funktion ändern. Folgende Standardvorgaben sind definierbar:





Die in den Grundeinstellungen definierte RFID Verwendungsart wirkt sich nur bei der Neuanlage von ekey net FS RFID aus. Individuelle Einstellungen an bestehenden Fingerscannern werden nicht aktualisiert. Kapitel 6.6.3.2.3

© 2010 – ekey biometric systems GmbH



ISO15693	☑ Ja

Die RFID-Terminals unterstützen die ISO15693 Norm. Die hier getroffene Einstellung gilt dann für alle RFID-Terminals im System.

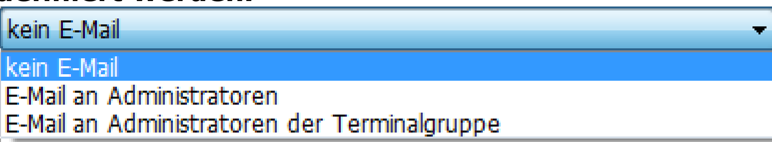
BUSINESS

8.1.1.3 BENACHRICHTIGUNGEN

Bei Auftreten der nachfolgend gelisteten Ereignisse werden automatische E-Mails an die definierten Empfänger gesandt. Die Einträge hier gelten als Standard-Vorgabe.

Masterserver Start	E-Mail an Administratoren
TOCAnet Terminalserver Start	E-Mail an Administratoren der Terminalgruppe
TOCAnet Terminalserver offline	E-Mail an Administratoren der Terminalgruppe
CONVERTER LAN offline	E-Mail an Administratoren der Terminalgruppe
Terminal offline	E-Mail an Administratoren der Terminalgruppe
Terminal Kommunikationsprobleme	E-Mail an Administratoren der Terminalgruppe
Terminal erster Schaltvorgang eines Tages	kein E-Mail
Terminal jeder Schaltvorgang	kein E-Mail
Terminal jeder Zutrittsversuch	kein E-Mail

Folgende Bedingungen für den E-Mail-Versand können für jedes auftretende Ereignis definiert werden.



- kein E-Mail beim auftretenden Ereignis wird kein E-Mail versandt.
- E-Mail an Administratoren: Alle Administratoren erhalten ein Email mit derBeschreibung des entsprechenden Ereignisses.
- E-Mail an Administratoren der Terminalgruppe: Nur die der Terminalgruppezugeordneten Administratoren erhalten die Benachrichtigung. (siehe dazu auch den Bereich „Rechte")

Die Einträge hier gelten als Vorgabe „Standard". Wo immer Sie dann im System , z. B. bei

- ekey net Terminalserver
- ekey net CV LAN
- ekey net FS

die Eigenschaften für Benachrichtigungen auf „Standard" setzen, gelten die Einstellungen die Sie hier machen.

BUSINESS

E-Mail nach Fehlerbehebung:

E-Mail nach Fehlerbehebung	Ja

Nachdem ein Terminal aus dem OFFLINE – Modus wieder in den ONLINE-Modus wechselt wird ein Email an den Administrator gesandt.

BUSINESS

SMTP-E-Mailserver

SMTP E-Mailserver	

Hostname oder Adresse des Postausgangs – Servers hier eintragen

Absender E-Mailadresse	

Die Emailadresse des Absenders, in diesem Fall von ekey net ist hier zu definieren.

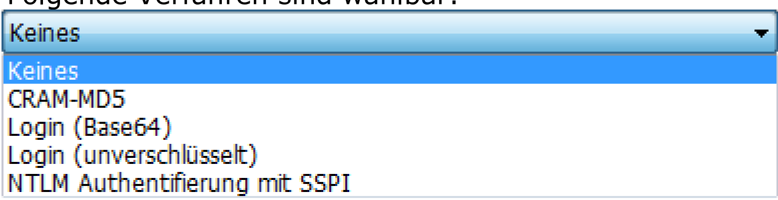


Sie können an ekey net kein Email senden! Die hier eingegebene Adresse hilft ihnen, wenn Sie eine für sich sprechende Adresse wählen,in ihrem Posteingangsordner klar zu erkennen, von wem die Email kommt.

SMTP Anmeldeverfahren:

SMTP Anmeldeverfahren	Keines

Wählen Sie das korrekte Verschlüsselungsverfahren Ihres SMTP - Servers aus
Folgende Verfahren sind wählbar:





Die Einstellungen für die E-mail-Funktionen, speziell im Hinblick auf SMTP –Servers sind abhängig von ihrer Systemkonfiguration. ekey kann ihnen in diesem Bereich nureingeschränkt Unterstützung bieten. Wenn Sie diese Funktionen aktivieren möchten, ziehen Sie bitte ihre IT-Spezialisten für die Konfiguration zu Rate.

SMTP Anmeldenamen:

SMTP Anmeldename	

Wenn erforderlich - bei den meisten SMTP Servern kann dieses Feld leer bleiben

SMTP Anmeldekennwort:

SMTP Anmeldekennwort	

Wenn erforderlich - bei den meisten SMTP Servern kann dieses Feld leer bleiben

BUSINESS

8.1.1.4 KALENDER

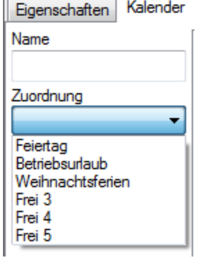
Geben Sie hier zusätzliche Zuordnungs-Bezeichnungen für die Kalendereigenschaften an (leer = nicht in Verwendung). Beispiele: Betriebsurlaub, Ferien, Tag der offenen Tür, Mitarbeiterabend,...

Benutzerdefinierter Kalender 1	Betriebsurlaub
Benutzerdefinierter Kalender 2	Weihnachtsferien
Benutzerdefinierter Kalender 3	
Benutzerdefinierter Kalender 4	
Benutzerdefinierter Kalender 5	

BUSINESS



Legen Sie im Bereich „**Terminals**" einen neuen Kalender an, können Sie unter Zuordnung die hier gemachten Einträge zuweisen.



8.1.2 Aktionen

Aktionen werden von ekey net immer nach einem vorher aufgetretenen Ereignis ausgeführt. Eine Aktion wird also von ekey net veranlasst. Im Gegensatz zum Ereignis: Beim Ereignis erfolgt eine Eingabe ins System.Bei der Auslieferung von ekey net sind bereits eine Reihe von möglichen Aktionen vordefiniert. Sie können aber auch selbst weitere Aktionen definieren.
Hier werden die Aktionen nur definiert, damit sie im System bekannt sind. Sie müssen diese Aktionen dann einem Ereignis zuweisen, damit diese zur Ausführung kommen. Siehe dazu auch Kapitel 8.1.3.

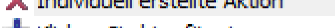
 *Bei denLizenzversionen* LIGHT *und* COM *gibt es keine Aktionen!*

Hier sehen Sie die Liste der vordefinierten BUSINESS Aktionen (diese sind nicht veränderbar):

Vorhandene Aktionen	
Impuls Anschluss 1	Sende 'Zutritt' zugeordnetes Gerät/Anschluss 1 3000ms Impuls
Impuls Anschluss 2	Sende 'Zutritt' zugeordnetes Gerät/Anschluss 2 3000ms Impuls
Impuls Anschluss 3	Sende 'Zutritt' zugeordnetes Gerät/Anschluss 3 3000ms Impuls
Impuls Anschluss 4	Sende 'Zutritt' zugeordnetes Gerät/Anschluss 4 3000ms Impuls
Anschluss 1 ein	Sende 'Zutritt' zugeordnetes Gerät/Anschluss 1 ein
Anschluss 2 ein	Sende 'Zutritt' zugeordnetes Gerät/Anschluss 2 ein
Anschluss 3 ein	Sende 'Zutritt' zugeordnetes Gerät/Anschluss 3 ein
Anschluss 4 ein	Sende 'Zutritt' zugeordnetes Gerät/Anschluss 4 ein
Anschluss 1 aus	Sende 'Verlassen' zugeordnetes Gerät/Anschluss 1 aus
Anschluss 2 aus	Sende 'Verlassen' zugeordnetes Gerät/Anschluss 2 aus
Anschluss 3 aus	Sende 'Verlassen' zugeordnetes Gerät/Anschluss 3 aus
Anschluss 4 aus	Sende 'Verlassen' zugeordnetes Gerät/Anschluss 4 aus
Anschluss 2 ein, LED ein	Sende 'Alarm ein' zugeordnetes Gerät/Anschluss 2 ein
Anschluss 3 ein, LED ein	Sende 'Benutzermodus 1' zugeordnetes Gerät/Anschluss 3 ein
Anschluss 4 ein, LED ein	Sende '' zugeordnetes Gerät/Anschluss 4 ein
Anschluss 2 aus, LED aus	Sende 'Alarm aus' zugeordnetes Gerät/Anschluss 2 aus
Anschluss 3 aus, LED aus	Sende 'Benutzermodus aus' zugeordnetes Gerät/Anschluss 3 aus
Anschluss 4 aus, LED aus	Sende '' zugeordnetes Gerät/Anschluss 4 aus
Anschluss 1 Umschalten	Sende 'Umschalten' zugeordnetes Gerät/Anschluss 1 umschalten
Anschluss 2 Umschalten	Sende 'Umschalten' zugeordnetes Gerät/Anschluss 2 umschalten
Anschluss 3 Umschalten	Sende 'Umschalten' zugeordnetes Gerät/Anschluss 3 umschalten
Anschluss 4 Umschalten	Sende 'Umschalten' zugeordnetes Gerät/Anschluss 4 umschalten
Ablehnung unbekannter Finger	Sende 'Unbekannter Finger'
Ablehnung bekannter Finger	Sende 'Ablehnung'
Reboot des Moduls	Sende 'Reboot Modul'
Impuls lokaler Anschluss 1	Sende 'Zutritt' Anschluss 1 3000ms Impuls
lokaler Anschluss 1 ein	Sende 'Zutritt' Anschluss 1 ein
lokaler Anschluss 1 aus	Sende 'Verlassen' Anschluss 1 aus
lokaler Anschluss 1 Umschalten	Sende 'Umschalten' Anschluss 1 umschalten
Verbund SE Impuls Anschluss 1	Sende 'Zutritt'
Verbund SE Impuls Anschluss 2	Sende 'Zutritt'
Verbund SE Impuls Anschluss 3	Sende 'Zutritt'
Verbund SE Impuls Anschluss 4	Sende 'Zutritt'
Verbund SE Impuls Anschluss 5	Sende 'Zutritt'
Verbund SE Impuls Anschluss 6	Sende 'Zutritt'



Verbund SE Impuls Anschluss 7	Sende 'Zutritt'
Verbund SE Impuls Anschluss 8	Sende 'Zutritt'
Verbund SE Impuls Anschluss 9	Sende 'Zutritt'
Verbund SE Impuls Anschluss 10	Sende 'Zutritt'
Verbund SE Impuls Anschluss 11	Sende 'Zutritt'
Verbund SE Impuls Anschluss 12	Sende 'Zutritt'
Verbund SE Impuls Anschluss 13	Sende 'Zutritt'
Verbund SE Impuls Anschluss 14	Sende 'Zutritt'
Verbund SE Impuls Anschluss 15	Sende 'Zutritt'
Verbund SE Impuls Anschluss 16	Sende 'Zutritt'
Verbund SE Impuls Anschluss 17	Sende 'Zutritt'
Verbund SE Impuls Anschluss 18	Sende 'Zutritt'
Verbund SE Impuls Anschluss 19	Sende 'Zutritt'
Verbund SE Impuls Anschluss 20	Sende 'Zutritt'
Verbund SE Impuls Anschluss 21	Sende 'Zutritt'
Verbund SE Impuls Anschluss 22	Sende 'Zutritt'
Verbund SE Impuls Anschluss 23	Sende 'Zutritt'
Verbund SE Impuls Anschluss 24	Sende 'Zutritt'
Verbund SE Impuls Anschluss 25	Sende 'Zutritt'
Verbund SE Impuls Anschluss 26	Sende 'Zutritt'
Verbund SE Impuls Anschluss 27	Sende 'Zutritt'
Verbund SE Impuls Anschluss 24	Sende 'Zutritt'
Verbund SE Impuls Anschluss 25	Sende 'Zutritt'
Verbund SE Impuls Anschluss 26	Sende 'Zutritt'
Verbund SE Impuls Anschluss 27	Sende 'Zutritt'
Verbund SE Impuls Anschluss 28	Sende 'Zutritt'
Individuell erstellte Aktion	Sende 'Verlassen'



Klicken Sie hier für einen neuen...

Aktion bearbeiten

Beschreibung	Individuell erstellte Aktion
Aktionscode	Verlassen
Gerät	Kein Gerät

8.1.2.1 Anlage benutzerdefinierter Aktionen

Natürlich haben Sie die Möglichkeit eigene Aktionen zu definieren, indem Sie
+ Klicken Sie hier für einen neuen...
wählen und folgende Einstellungen anpassen:

Hier ein Beispiel:

Aktion bearbeiten	
Beschreibung	Impuls Anschluß 1
Aktionscode	Zutritt
Gerät	Zugeordnetes Gerät - Anschluß 1
Schaltmodus	Impuls
Selbsthaltung erlauben	☑ Ja
Impulsdauer (ms)	3000
LED (einfärbig)	Unverändert
LED (dreifärbig)	Unverändert

Beschreibung:

Beschreibung	Neue Aktion

Benennen Sie die Aktion so aussagekräftig, dass klar ist welche Handlung ekey net mit dieser Aktion ausführt.

Aktionscode:

Aktionscode	Kein Aktionscode

Die Bezeichnung dieses gewählten Eintrages wird bei Logging - Funktionen verwendet.
Folgende Aktionscodes können gewählt werden:

Kein Aktionscode
- Kein Aktionscode
- Zutritt
- Verlassen
- Ablehnung
- Unbekannter Finger
- Alarm ein
- Alarm aus
- Alarmstufe aus
- Alarmstufe 1
- Alarmstufe 2
- Alarmstufe 3
- Benutzermodus aus
- Benutzermodus 1
- Benutzermodus 2
- Benutzermodus 3
- Reboot Modul
- Umschalten

Kein Aktionscode: Wählen Sie diesen Eintrag, so erfolgt bei Ausführung einer solchen Aktion kein Log-Eintrag.
Zutritt: Finger wurde erkannt und besitzt die Berechtigung zum Zutritt. Dies führt zur Ausführung dieser Aktion.
Verlassen: Finger wurde erkannt und ist berechtigt zur Ereignisauslösung. Dies führt zur Ausführung dieser Aktion.

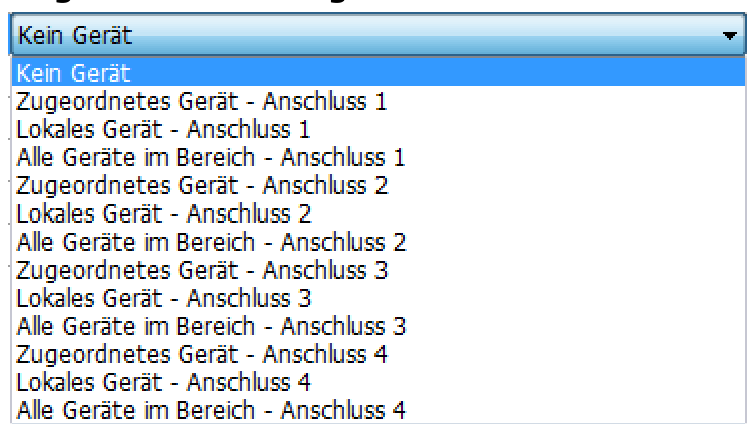
Ablehnung: Der Finger wird im System erkannt, allerdings besitzt er derzeit keine Berechtigung zum Zutritt (Zeitfenster oder Kalender lässt dies nicht zu). Tritt dies auf, so wird diese Aktion ausgeführt
Unbekannter Finger: Ein unbekannter Finger wurde über ein Terminal erfasst (über Sensor gezogen).Tritt dieses Ereignis auf, so wird diese Aktion ausgeführt.
Reboot Modul: Der Fingerscanner wird neugestartet
Benutzermodus 1,2 oder 3: Alle Geräte schalten das definierte Relais bis zur nächsten Bereichsgrenze und ändern die Berechtigungen abhängig zum zugehörigen Zeitfenster „Benutzermodus1,2 oder 3"(vordefiniert)
Benutzermodus aus: Das angezogene Relais von dem Benutzermodus wird wieder ausgeschaltet
Umschalten: Finger wurde erkannt und ist berechtigt zur Ereignisauslösung. Dies führt zur Ausführung dieser Aktion.

Gerät	Zugeordnetes Gerät - Anschluß 1

Sie definieren hier auf welchem Gerät die Aktion ausgeführt werden soll. Als Gerät ist in diesem Zusammenhang die ekey net SE zu verstehen. Die Bezeichnung „Anschluss" weist auf das entsprechende Schaltelement auf dem Gerät hin. z.B. die ekey net SE AP besitzt 3 Relais. Die Zuweisung heißt dann:

Anschluß 1 = Relais 1
Anschluß 2 = Relais 2
Anschluß 3 = Relais 3

Folgende Einstellungen sind wählbar:



Zugeordnetes Gerät:Jedem ekey net FS ist bei der Einbindung ins System in seinen Eigenschaften ein Gerätzuzuordnen. Wählen Sie nun „Zugeordnetes Gerät – Anschluss„1", so wird die hier definierte Aktion auf diesem zugeordneten Gerät auf Relais 1 (oder O1) ausgeführt. Analog gilt für:
„Zugeordnetes Gerät – Anschluß 2" -> Aktion auf Relais 2 (oder O2)
„Zugeordnetes Gerät – Anschluß 3" -> Aktion auf Relais 3 (oder O3)
„Zugeordnetes Gerät – Anschluß 4" -> Aktion auf Relais 4 (oder O4)

Lokales Gerät: Bei einem „lokalen Gerät" befindet sich das Schaltelement direkt auf dem ekey net FS (z.B. ekey net MFSUP REL). Dort muss natürlich beiden Eigenschaften des Terminals kein Gerät zugeordnet werden. Anschluss 1 – 4bedeutet Schaltelement 1 – 4. Die Aktion wirkt bei einer dieser Definitionen direkt auf die Anschlüsse am Fingerscanner.





Das verwendete Terminal (Fingerscanner) muß natürlich diese Anschlüsse auch ausgeführt haben. Prüfen Sie, ob der verwendete ekey net FS Relais bzw. IO-Ausgänge besitzt.

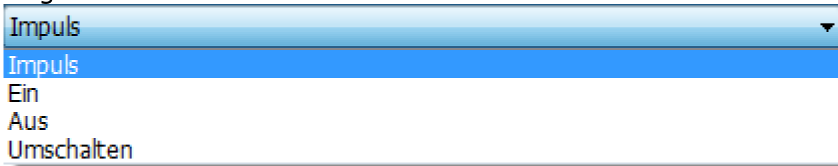
Alle Geräte im Bereich: Hier wird die Aktion auf alle Geräte (lokale und auch nicht zugeordnete) im definierten Bereich ausgeführt. Der Bereich definiert sich über Bereichsgrenzen. Diese Bereichsgrenze kann ein ekey net CVLAN, ein ekey net Terminalserver oder eineTerminalgruppe sein (Siehe dazu auch Kapitel 16 Bereichsgrenzen.).

Schaltmodus:

Schaltmodus	Impuls

Der Schaltmodus definiert auf welche Art und Weise das Schaltelement (Anschluss 1, 2, 3,…) auf dem vorher definiertem Gerät (Bereich, lokal, zugeordnet) arbeitet.

Folgende Modi können definiert werden



Impuls: Das Schaltelement macht eine Impulsschaltung. Das Relais schaltet ein und nach einerdefinierten Zeit wieder aus. Die Impulsdauer ist einstellbar (siehe nächsten Absatz).
Ein: das Schaltelement (Relais) wird eingeschalten (= Kontakt NO schließt bzw. der Ausganggeht auf HIGH) und verbleibt in diesem Zustand.
Aus: das Schaltelement (Relais) wird ausgeschalten (= Kontakt NO öffnet bzw. der Ausganggeht auf LOW) und verbleibt in diesem Zustand
Umschalten: das Schaltelement (Relais) wechselt seinen Zustand. War es eingeschalten, schaltet esbei Ausführung dieser Aktion aus, war es ausgeschalten, so schaltet es jetzt ein.

Selbsthaltung:

Selbsthaltung erlauben	☑ Ja

Die Selbsthaltungsfunktion im ekey net ist im Kapitel 6.6.6.1.2detailliert beschrieben. Der wesentliche Unterschied zum Schaltmodus EIN bzw. IMPULS (siehe Schaltmodus) ist, dass die Abschaltung in Abhängigkeit der Zeitfenstereinstellungen erfolgt. Hier definieren Sie, ob bei Ausführung der Aktion die Selbsthaltungsfunktion für das Schaltelement (Anschluss) wirksam ist oder nicht.

Impulsdauer:

Impulsdauer (ms)	3000

Wurde als Schaltmodus „Impuls" gewählt, so definieren Sie hier die Dauer des Schaltimpulses am Schaltelement (Anschluss) bei Ausführung der Aktion. Die Einstellungen hier sind für die Schaltmodi EIN, AUS und UMSCHALTENwirkungslos.

Einstellbereich:
100 = 0,1Sekunden
60000 = 60 Sekunden
Als Standardwert schlägt ekey net 3000ms vor (entspricht 3s). Damit ist ein Großteil der Türverriegelungen (Motorschloss,...) steuerbar.

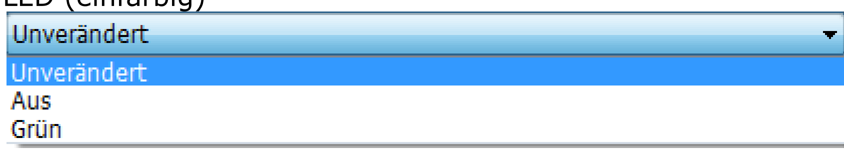
LED:
Verändern Sie die Anzeigen der LED´s bei den Fingerscannern

LED (einfärbig)	Unverändert
LED (dreifärbig)	Unverändert

LED (einfärbig) verfügbar bei folgenden Modellen: FS-AP (rechts)

LED (dreifärbig) verfügbar bei folgenden Modellen: integra (rechts)

LED (einfärbig)



LED(dreifärbig)

Unverändert

Unverändert
Aus
Grün
Rot
Gelb

8.1.2.2 Löschen von Aktionen

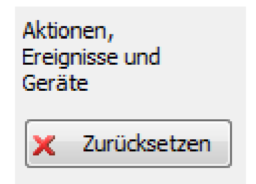
Aktionen können, wenn Sie keine Verwendung finden, auch gelöscht werden. ekey empfiehlt dies auch zu tun, da sich die Übersichtlichkeit des Systems verbessert und dadurch die Wartung einfacher und das Risiko von Fehlkonfigurationen minimiertwird. Wollen Sie eine Aktion löschen, so klickenSie auf das rote „X" neben der Aktion. Die Löschung erfolgt augenblicklich!

X Impuls Anschluß 1 Sende 'Zutritt' zugeordnetes Gerät/Anschluß 1 100ms Impuls



Achten Sie darauf, dass die Aktion wirklich nicht mehr verwendet wird. ekey net prüft dies nicht ab und löscht einfach die Aktion!Vordefinierte Aktionen können nicht gelöscht werden

8.1.2.3 Zurücksetzen von Aktionen



Durch Klicken auf den Button "Zurücksetzen" können alle Aktionen, Ereignisse und Geräte auf den Auslieferungszustand zurückgesetzt werden.



ACHTUNG - Alle von Ihnen angelegten und definierten Aktionen, Ereignisse und Geräte werden gelöscht und der Standard lt. Werkseinstellung wiederhergestellt.

8.1.3 Ereignisse

Ereignisse sind externe Eingaben in das ekey net - System, die zur Ausführung definierter Aktionen führen. Beispielsweise das Ziehen eines Fingers mit positiver Erkennung.Damit ist auch definiert, dass Aktionen (siehe Kapitel 8.1.2)einem Ereignis zugeordnet werden müssen. Ein Ereignis kann maximal 2 Aktionen auslösen. Diese beiden Aktionen können einerseits parallel ablaufen, andererseits kann das zweite Ereignis aber auch weiteren Abhängigkeiten folgen (z.B. Anzahl des Auftretens des Ereignisses, Timeouts usw).
Ereignisse werden bei der Fingeraufnahme (siehe Kapitel 6.4.2.2) dem Finger zugeordnet.Wird der entsprechendeFinger dann über den Sensor gezogen, so löst es damit das zugeordnete Ereignis aus und die Abarbeitung der Aktionen startet.



Bei den Lizenzversionen 

gibt es keine Ereignisse!

Im ekey net BUSINESS sind eine Reihe von Ereignissen wie folgt vordefiniert:

Externe Ereignisse	Aktion
Mit Finger Türe öffnen	Impuls Anschluss 1
Mit Finger Türe dauerhaft öffnen	Anschluss 1 ein
Mit Finger Türe dauerhaft sperren	Anschluss 1 aus
Mit Finger Alarmananlage ein	Anschluss 2 ein, LED ein
Mit Finger Alarmananlage aus	Anschluss 2 aus, LED aus
Mit Finger Anschluß 3 ein	Anschluss 3 ein
Mit Finger Anschluß 4 ein	Anschluss 4 ein
Anschluss 2 schalten	Impuls Anschluss 2
Anschluss 3 schalten	Impuls Anschluss 3
Anschluss 4 schalten	Impuls Anschluss 4
Anschluss 1 Umschalten	Anschluss 1 Umschalten
Anschluss 2 Umschalten	Anschluss 2 Umschalten
Anschluss 3 Umschalten	Anschluss 3 Umschalten
Anschluss 4 Umschalten	Anschluss 4 Umschalten



Ablehnung unbekannter Finger	Ablehnung unbekannter Finger
Ablehnung bekannter Finger	Ablehnung bekannter Finger
Mit Finger Türe öffnen (lokales Relais)	Impuls lokaler Anschluss 1
Mit Finger Türe dauerhaft öffnen (lokales Relais)	lokaler Anschluss 1 ein
Mit Finger Türe dauerhaft sperren (lokales Relais)	lokaler Anschluss 1 aus
Mit Finger Anschluss Umschalten (lokales Relais)	lokaler Anschluss 1 Umschalten
Verbund SE Anschluss 1 schalten	Verbund SE Impuls Anschluss 1
Verbund SE Anschluss 26 schalten	Verbund SE Impuls Anschluss 26
Verbund SE Anschluss 27 schalten	Verbund SE Impuls Anschluss 27
Verbund SE Anschluss 28 schalten	Verbund SE Impuls Anschluss 28
Individuell erstelltes Ereignis	lokaler Anschluss 1 aus
Klicken Sie hier für einen neuen Eintrag	

Externes Ereignis bearbeiten

Beschreibung	Individuell erstelltes Ereignis

Mit Finger Türe öffnen: Bei Auftreten des Ereignisses wird die Aktion eines 3- sekundigen Schaltimpuls auf Anschluss 1 ausgelöst.
Mit Finger Türe dauerhaft öffnen: Auftreten dieses Ereignisses schaltet den Anschluss 1 am zugehörenden Gerät dauerhaft ein
Mit Finger Türe dauerhaft sperren: Auftreten dieses Ereignisses schaltet den Anschluss 1 am zugehörenden Gerät dauerhaft aus.
Mit Finger Alarmanlage ein: Auftreten dieses Ereignisses schaltet den Anschluss 2 am zugehörenden Gerät dauerhaft ein, und schaltet LED (3-färbig)auf rot
Mit Finger Alarmanlage aus: Auftreten dieses Ereignisses schaltet den Anschluss 2 am zugehörenden Gerät dauerhaft aus und LED (3 färbig) aus.
Mit Finger Anschluß 3 ein: Auftreten dieses Ereignisses schaltet den Anschluss 3 am zugehörenden Gerät dauerhaft ein
Mit Finger Anschluß 4 ein: Auftreten dieses Ereignisses schaltet den Anschluss 4 am zugehörenden Gerät dauerhaft ein
Anschluß 2 schalten: Bei Auftreten des Ereignisses wird die Aktion eines 3- sekundigen Schaltimpuls auf Anschluss 2 ausgelöst.
Anschluß 3 schalten: Bei Auftreten des Ereignisses wird die Aktion eines 3- sekundigen Schaltimpuls auf Anschluss 3 ausgelöst.
Anschluß 4 schalten: Bei Auftreten des Ereignisses wird die Aktion eines 3- sekundigen Schaltimpuls auf Anschluss 4 ausgelöst.
Anschluss 1 umschalten: Auftreten dieses Ereignisses schaltet den Anschluss 1 am zugehörenden Gerät um (Das Relais schalten in den anderen Zustand -> AUS wird EIN).
Anschluss 2 umschalten: Auftreten dieses Ereignisses schaltet den Anschluss 2 am zugehörenden Gerät um (Das Relais schaltet in den anderen Zustand -> AUS wird EIN).
Anschluss 3 umschalten: Auftreten dieses Ereignisses schaltet den Anschluss 3 am zugehörenden Gerät um (Das Relais schaltet in den anderen Zustand -> AUS wird EIN).
Anschluss 4 umschalten: Auftreten dieses Ereignisses schaltet den Anschluss 4 am zugehörenden Gerät um (Das Relais schaltet in den anderen Zustand -> AUS wird EIN).
Ablehnung unbekannter Finger: ein am Fingerscanner unbekannter Finger wurde am Terminal abgelehnt. Es wird keine weitere Aktion ausgelöst.
Ablehnung bekannter Finger: ein am Fingerscanner bekannter Finger wurde abgelehnt (aufgrund fehlender Berechtigung). Es wird keine weitere Aktion ausgelöst.
Mit Finger Türe öffnen(lokales Relais): Bei Auftreten des Ereignisses wird die Aktion eines 3- sekundigen Schaltimpuls auf dem lokalen Anschluss am ekey net FS ausgelöst.



Mit Finger Türe dauerhaft öffnen(lokales Relais): Auftreten dieses Ereignisses schaltet den lokalen Anschluss am ekey net FS dauerhaft ein
Mit Finger Türe dauerhaft sperren(lokales Relais): Auftreten dieses Ereignisses schaltet den lokalen Anschluss am ekey net FS dauerhaft aus.
Mit Finger Anschluss umschalten(lokales Relais): Auftreten dieses Ereignisses schaltet den lokalen Anschluss am ekey net FS um (Das Relais schaltet in den anderen Zustand -> AUS wird EIN).
Verbund SE Anschluss „X" schalten: Bei Auftreten des Ereignisses wird die Aktion eines 3-sekundigen Schaltimpuls auf dem zugewiesenen Verbund Anschluss X ausgelöst. Möglich von Anschluss 1 bis Anschluss 28 – siehe Kapitel 6.6.3.2.2



Damit Sie dieses Ereignis definieren können, muss ihr Fingerscanner natürlich auch einen lokalen Anschluss (Relais) besitzen.



Die beiden Ablehnungs – Ereignisse von bekannten und unbekannten Fingern beziehen sich immer auf die Daten am einzelnen Fingerscanner. Bei z.B. „Ablehnung unbekannter Finger" heißt dies, dass der Finger an dem speziellen Fingerscanner nicht erfasst ist. Er kann aber sehr wohl an einem anderen Fingerscanner im System erfasst sein.



Die Ablehnungs-Ereignisse führen in der Standardkonfiguration zu keiner direkten Schaltaktion. Sie können aber durchaus auch eine andere Aktion zuweisen(siehe dazu „benutzerdefinierte Ereignisse" weiter unten im Kapitel). z.B. Anschluss 2 schalten und dort eine Kamera anbinden. So können Sie z.B. einen Fotonachweis über eine unberechtigte Bedienung ihres Systems machen.

8.1.3.1 Anlage benutzerdefinierter Ereignisse

Natürlich haben Sie die Möglichkeit eigene Ereignisse zu definieren, indem Sie
+ Klicken Sie hier für einen neuen Eintrag
wählen und folgende Einstellungen anpassen:

<u>Beschreibung:</u>

Beschreibung	Mit Finger Türe öffnen

benennen Sie das Ereignisso aussagekräftig, dass klar ist, welche Eingabe von extern ins System erfolgt.

<u>Aktion:</u>

Aktion	Impuls Anschluß 1

Wählen Sie aus den vordefinierten oder erstellten Aktionen die gewünschte aus. Aktionen können ebenfallsfrei definiert werden (siehe dazu Kapitel 0).Diehier gewählte Aktion wird dann bei Auftreten des Ereignisses ausgeführt.

<u>Zähler:</u>

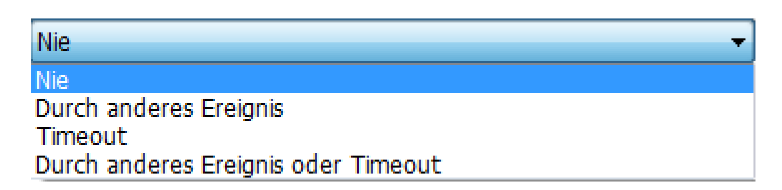
Zähler	2

Ein Ereignis kann auch 2 Aktionen auslösen. Der Zähler definiert nun den Zeitpunkt des Auslösens der„Aktion bei Zählerende"(= 2. Aktion). Der eingestellte Zählerwert bedeutet, dass das Ereignis der eingestellten Anzahldes Zählerwertes entsprechend auftreten muss, damit die „Aktion bei Zählerende" ausgelöst wird.
Einstellungsbereich: 1 …100
Wird 1 oder 0 eingestellt, so werden „Aktion" und „Aktion bei Zählerende" immer parallel ausgeführt.

Rücksetzen:



Rücksetzen bezieht sich auf den zuvor genannten Zähler. Wird die „Aktion bei Zählerende“ ausgeführt, so wird der Zähler automatisch auf 0 zurückgesetzt. Zusätzlich kann der Zähler aber auch aufgrund folgender Bedingungen zurückgesetzt werden:



Wird der Zähler zurückgesetzt, erfolgt keine Ausführung der „Aktion bei Zählerende“
Nie: Zählerwert wird nur bei „Zählerende“ rückgesetzt, d.h. wenn das Ereignis so oft aufgetreten ist, wie es im Zähler definiert wurde.
Durch anderes Ereignis: tritt irgendein anderes am ekey net FS definiertes Ereignis auf,wird der Zählerzurückgesetzt.
Timeout: Der Zähler kann auch nach einer bestimmten Zeit rückgesetzt werden. Die Zeit ist im nächstfolgenden Eingabefeld „Timout in Sekunden“ zu definieren.
Durch anderes Ereignis oder Timeout: Auch die Kombination von anderem Ereignis und Timeout ist möglich.



Das Ereignis muss am gleichen ekey net FS (Terminal) entsprechend der Anzahl auftreten damit Aktion bei Zählerende ausgeführt wird. Gleiches gilt auch für das Rücksetzenbei Zählerende. Wie oft generell das Ereignis im ganzen System (Es könnte ja auf mehreren Fingerscannern das Ereignis auftreten) ausgeführt wird, ist irrelevant.

Timeout in Sekunden

Timeout in Sekunden	0

Diese Einstellung bezieht sich nun auf die Art des Rücksetzens des Zählers. Wurde im Eingabefeld „Rücksetzen“

- Timeout bzw.
- Durch anderes Ereignis oder Timeout

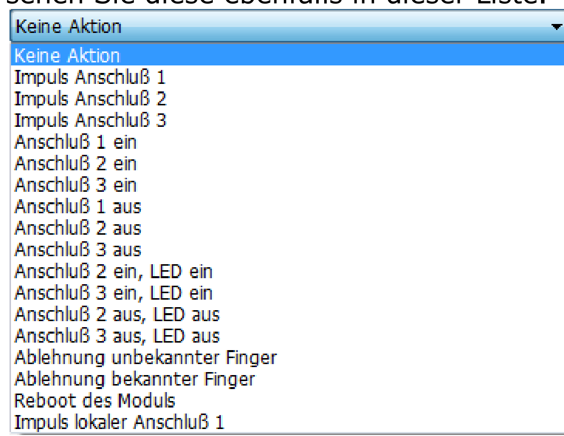
definiert, so ist hier diese Timeout-Zeit zu definieren, nach deren Ablauf der Zähler zurückgesetzt wird. Der Einstellbereich bewegt sich von 1 – 3600 Sekunden

Aktion bei Zählerende:

Aktion bei Zählerende	Keine Aktion

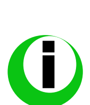
Tritt das Ereignis entsprechend der definierten Anzahl (lt. Zähler) auf, ohne dass es zu einem Rücksetzen kommt, so wird diese Aktion ausgeführt. Wählen Sie aus den vordefinierten oder erstellten Aktionen die gewünschte aus. Aktionen können ebenfallsfrei definiert werden (siehe dazu Kapitel 0)

Als Beispiel sehen Sie hier eine Aktionsliste. Haben Siebenutzerdefinierte Aktionen erstellt, so sehen Sie diese ebenfalls in dieser Liste.





Aktionen die auf Bereiche wirken, dürfen hier nicht definiert werden.Lesen Sie dazu unbedingt Kapitel 16.4



<u>Praxisbeispiel für das Arbeiten mit Zähler:</u> Nach 3 fehlerhaften Zutrittsversuchen innerhalb von 2 Minuten, soll die Alarmkamera aktiviert werden, um den versuchten "Einbruch" zu filmen. Ist innerhalb der 2 Minuten ein Finger erkannt worden, so ist der Zähler zurückzusetzen. Die Alarmkamera wird durch einen Impuls auf Anschluss 2 ausgelöst.Die Einstellung für dieses Ereignis sieht wie folgt aus:

<u>Ereigniscode:</u>

Externes Ereignis bearbeiten	
Beschreibung	Alarmkamera
Aktion	Ablehnung unbekannter Finger
Zähler	3
Rücksetzen	Durch anderes Ereignis oder Timeout
Timeout in Sekunden	120
Aktion bei Zählerende	Impuls Anschluß 2
Ereigniscode	

Ereigniscode

Frei definierbarer Text - max. 15 Zeichen - für externe Programme. Diese Information wird via UDP-Block vom Terminalserver versendet.



Testen Sie neue Ereignisse vor dem Einsatz in ihrem Echtsystem in einer separaten Testumgebung.

© 2010 – ekey biometric systems GmbH



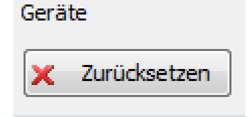
8.1.3.2 Löschen von Ereignissen

Ereignisse können, wenn Sie keine Verwendung finden, auch gelöscht werden. ekey empfiehlt dies auch zu tun, da sich die Übersichtlichkeit des Systems verbessert und dadurch die Wartung einfacher und das Risiko von Fehlkonfigurationen minimiert wird.
Wollen Sie ein Ereignis löschen, so klickenSie auf das rot „**X**" neben dem Ereignis. Die Löschung erfolgt augenblicklich!

Mit Finger Türe dauerhaft öffnen   Anschluß 1 ein



Achten Sie darauf, dass das Ereignis wirklich nicht mehr verwendet wird. ekey net prüft dies nicht ab und löscht einfach das Ereignis!



8.1.3.3 Zurücksetzen von Ereignissen

Durch Klicken auf den Button "Zurücksetzen" können alle Aktionen, Ereignisse und Geräte auf den Auslieferungszustand zurückgesetzt werden.

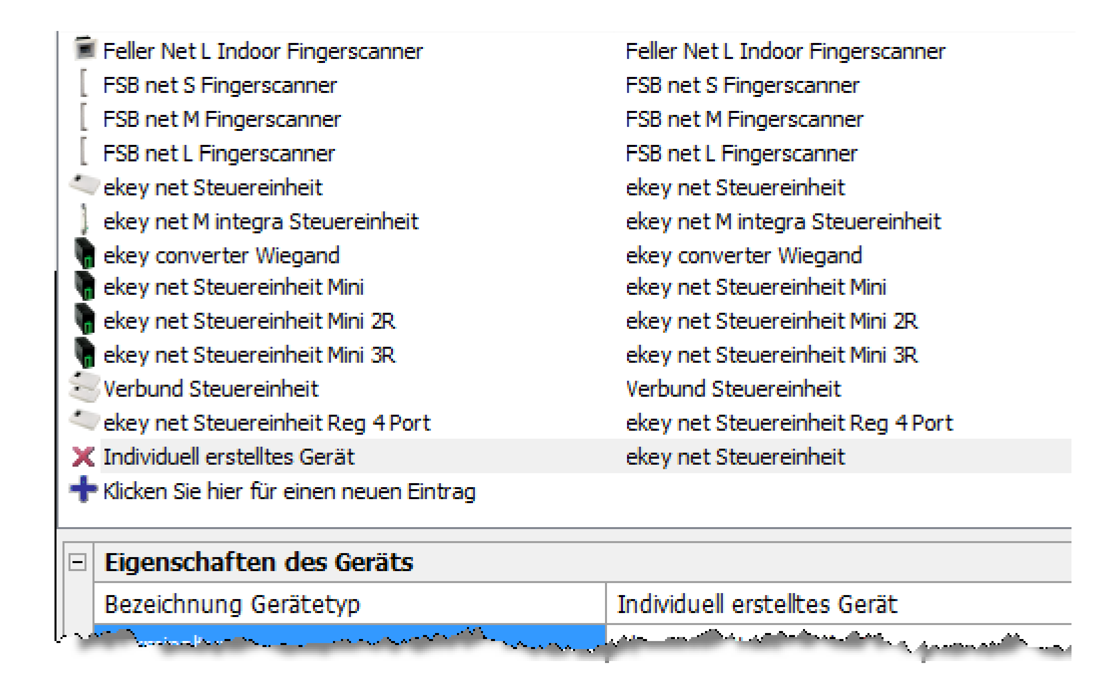


ACHTUNG - Alle von Ihnen angelegten und definierten Aktionen, Ereignisse und Geräte werden gelöscht und der Standard lt. Werkseinstellung wiederhergestellt -**ACHTUNG**

8.1.4 Geräte (Gerätetypen)

Geräte sind ekey net FS (Sensoreinheit -> Erfassung des Fingerprints) und ekey netSE (Aktoreinheiten -> Ausführen von Aktionen), welche auf Basis der definierten Aktionen und Ereignisse agieren.In diesem Kapitel erfahren Sie wie Sie neue **Gerätetypen**definieren, die abweichendes Verhalten zu den Standardgeräten zeigen.Diese Gerätetypendefinieren dann die Eigenschaften der Fingerscanner und SE im System.
Im ekey net sind eine ganze Reihe von Gerätetypen vordefiniert. Diese vordefinierte Gerätetypenliste sehen Sie hier:

Gerätevorlagen	Terminaltype
ekey net S Fingerscanner	ekey net S Fingerscanner
ekey net S integra Fingerscanner	ekey net S integra Fingerscanner
ekey net S RFID-Fingerscanner	ekey net S RFID-Fingerscanner
ekey net M Fingerscanner	ekey net M Fingerscanner
ekey net M integra Fingerscanner	ekey net M integra Fingerscanner
ekey net M RFID-Fingerscanner	ekey net M RFID-Fingerscanner
ekey net L Fingerscanner	ekey net L Fingerscanner
ekey net L integra Fingerscanner	ekey net L integra Fingerscanner
ekey net L RFID-Fingerscanner	ekey net L RFID-Fingerscanner
Feller Net S Fingerscanner	Feller Net S Fingerscanner
Feller Net S Indoor Fingerscanner	Feller Net S Indoor Fingerscanner
Feller Net M Fingerscanner	Feller Net M Fingerscanner
Feller Net M Indoor Fingerscanner	Feller Net M Indoor Fingerscanner
Feller Net L Fingerscanner	Feller Net L Fingerscanner





Die oben genannte Liste der vordefinierten Gerätetypen spiegelt der Stand zum Zeitpunkt derErstellung dieses Handbuches wider. Es kommen im Laufe der Zeit immer wieder neue Gerätetypen dazu. Klären Sie mit ekey direkt, welche Gerätetypen voreingestellt zur Verfügung stehen. Dieoben genannteListe ist für die Lizenzversion BUSINESS gültig. In den Versionen LIGHT und COM ist die Liste entsprechend eingeschränkt.

8.1.4.1 Anlage benutzerdefinierter Geräte



Bei den Lizenzversionen LIGHT und COM gibt es keine benutzerdefinierten Geräte!

8.1.4.1.1 Allgemein

In diesem Abschnitt können Sie spezielle Gerätetypen definieren. Hier geht es noch nicht darum Geräte bereits im System in Betrieb zu nehmen.Sie können für ihre Anwendung die vordefinierten Gerätetypen verwenden, haben aber auch die Möglichkeit Gerätetypen an ihre eigenen Bedürfnisse anzupassen.Ein neues Gerät ist nur eine bestehende Type (bereits vordefiniertes Gerät) mit neuen modifizierten Funktionen in Teilbereichen.Sie können hier **nicht** z.B. aus einem ekey net M Fingerscanner (200 Finger) einen ekey net L Fingerscanner mit z.B. 2000 Finger machen. Die variablen Funktionen,die Sie hier einem neuen Gerät zuweisen können, beschränken sich auf:

Bei ekey net FS:

Ereigniszuordnung
Ereignisumwandlung

Bei ekey net FS RFID:

Ereigniszuordnung
Ereignisumwandlung
RFID-Parameter

Bei ekey net SE: Geräteanschlüsse (Anschlussbezeichnungen)

ekey net CV WIEG: Wiegand-Optionen

Nur auf Basis dieser Parameterkönnen Sie neue Gerätetypen erstellen, die von den Standardgeräten abweichen.



Benutzerdefinierte Gerätetypen können nur in der Lizenzversion „BUSINESS" angelegt werden.

8.1.4.1.2 Neuen Gerätetyp anlegen

Für die Anlage benutzerdefinierter Gerätetypen klicken Sie unter Gerätevorlagen auf

➕ Klicken Sie hier für einen neuen Eintrag

Für jeden Gerätetyp müssen Sie folgende 2 Eingaben definieren:

Bezeichnung Gerätetyp:

Bezeichnung Gerätetyp	Neues Gerät

Geben Sie hier einen sprechenden Namen für den neuen Gerätetyp ein.

Terminaltype:

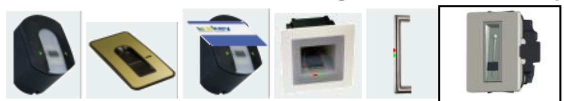
Terminaltype	ekey net M Steuereinheit

Terminaltype definiert welche Grundfunktion das neue Gerät hat. Damit wird hier ein Standardgerät zugewiesen. Diese Zuweisung definiert welche Grundfunktion ihr Gerät hat bzw. welche Geräteart vorliegt. Sie müssen also wissen, welches Produkt Sie vor sich haben, das Sie mit den neuen Parametern betreiben wollen. Die Gerätebezeichnung und die Artikelnummer können Sie auf der Seriennummernetikette des Produktes ablesen. Hier die Liste der möglichen Gerätetypen

ekey net Steuereinheit Reg 4 Port ▾

ekey net S Fingerscanner
ekey net S integra Fingerscanner
ekey net S RFID-Fingerscanner
ekey net M Fingerscanner
ekey net M integra Fingerscanner
ekey net M RFID-Fingerscanner
ekey net L Fingerscanner
ekey net L integra Fingerscanner
ekey net L RFID-Fingerscanner
Feller Net S Fingerscanner
Feller Net S Indoor Fingerscanner
Feller Net M Fingerscanner
Feller Net M Indoor Fingerscanner
Feller Net L Fingerscanner
Feller Net L Indoor Fingerscanner
FSB net S Fingerscanner
FSB net M Fingerscanner
FSB net L Fingerscanner
ekey net Steuereinheit
ekey net M integra Steuereinheit
ekey converter Wiegand
ekey net Steuereinheit Mini
ekey net Steuereinheit Mini 2R
ekey net Steuereinheit Mini 3R
Verbund Steuereinheit
ekey net Steuereinheit Reg 4 Port

8.1.4.1.3 Einstellungen für neue Typen ekey netFS



8.1.4.1.3.1 Eigenschaften des Gerätes

Rechte LED:

Rechte LED	Verbunden/Nicht verbunden

Diese Funktion ist nur bei den ekey Fingerscannern wirksam.
Die rechte LED der ekey net FS kann für kundenspezifische Anzeigen verwendet werden
Folgende Möglichkeitender Konfiguration gibt es:

Verbunden/Nicht verbunden
Verbunden/Nicht verbunden
In Aktionen verwendbar

Verbunden / Nicht verbunden: zeigt an, ob der Fingerscanner eine ordentliche Datenverbindung zum ekey net Terminalserver hat. Ist die Verbindung unterbrochen, geht die LED aus.
In Aktionen verwendbar: In diesem Fall wird die LED in Abhängigkeit der auszuführenden Aktion aktiviert bzw. deaktiviert. Einer Aktion geht immer ein Ereignis voraus.(siehe auch Kapitel8.1.2)

8.1.4.1.3.2 RFID - Die folgenden Einstellungen gelten nur für die ekey net FS RFID



Standard RFID Einstellungen verwenden:

Standard RFID-Einstellungen verwenden	☐ Nein

Wird hier „Ja" gewählt so gelten die Einstellungen wie im Reiter „Optionen" (siehe Kapitel **8.1.1**) definiert. Bei „NEIN" können hier für diese Fingerscannertype die Konfigurationen abweichend zum Standard definiert werden. Diese Einstellungen beziehen sich auf die möglichen Kommunikationsprotokolle (= RFID-Karte), die der Fingerscanner erkennen soll.

ISO15693	☑ Ja

Treffen Sie hier ihre Auswahl.



Sie können hier Abweichungen zum Standard machen, wir empfehlen Ihnen aber grundsätzlich immer vom Standard auszugehen. Das System bleibt damit übersichtlicher.

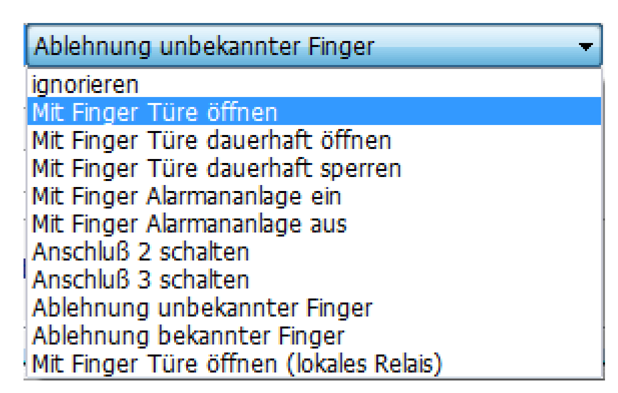
8.1.4.1.3.3 Ereigniszuordnungen

Ereignis bei Ablehnung unbekannter Finger:

Ereignis bei Ablehnung unbekannter Finger	Ablehnung unbekannter Finger

Der neue vordefinierte Fingerscanner kann bei einem unbekannten Finger ein entsprechendes Ereignis auslösen. Dieses Ereignis ist hier auszuwählen. In der Liste können aber auch eventuell von ihnen speziell definierte Ereignisse gelistet sein. Bei Auslieferung sind folgende Ereignisse auswählbar:



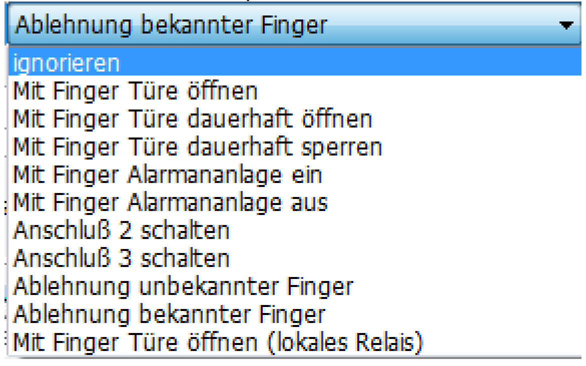


Bei den Standardgeräten ist das Ereignis „Ablehnung unbekannter Finger" vordefiniert

Ereignis bei Ablehnung bekannter Finger:

Ereignis bei Ablehnung bekannter Finger	Ablehnung bekannter Finger

Wird ein im ekey net bekannter Finger über den Sensor gezogen und dieser auch erkannt, so kann es trotzdem sein, dass er aufgrund einer Zeit oder Kalendereinschränkung abgelehnt wird. Passiert dies, so wird das hier definierte Ereignis ausgelöst.



Bei den Standardgeräten ist das Ereignis „Ablehnung bekannter Finger" vordefiniert

8.1.4.1.3.3.1 Die folgenden Einstellungen gelten nur für die Feller net M(S,L) FS



Bezeichnung Statuseingang 1:

Bezeichnung Statuseingang 1	Türstatus 1

Der Feller net M(S,L) FS hat einen digitalen Eingang, über den z.B. der Türstatus (Tür offen bzw. Tür geschlossen) ins System eingelesen werden kann. Die Bezeichnung für diesen Eingang ist hier zu definieren. Der Zustand des Einganges kann im Gerätestatus abgefragt werden und weiter können Sie, wenn Sie ein Logging aktivieren, Statusänderungen dieses Einganges in den entsprechenden Log-Files protokollieren und dann nachvollziehen.



Vergeben Sie hier einen sprechenden Namen wie z.B. „Lagertüre 1". Mit dieser Bezeichnung erkennen Sie dann sofort den zugehörigen Logeintrag.



8.1.4.1.3.3.2 Die folgenden Einstellungen gelten nur für den Feller net M(S,L) FS REL



Anschluss 1:

Anschluß 1	Ausgang/Relais

Beim Feller net FS REL steht am Fingerscanner selbst ein zusätzliches Schaltrelais zur Verfügung. Die Bezeichnung (Name) für dieses Relais können Sie hier definieren.



Verwenden Sie das interne Relais am Fingerscanner zur Öffnung der Türen, haben Sie eine Einschränkung der Sicherheit. Wir empfehlen aus diesem Grund diese Art der Züransteuerung über das interne Relais des Fingerscanners nur im Innenbereich für rein organisatorische Zutritts-Beschränkungen zu verwenden!!

8.1.4.1.3.4 Ereignis Umwandlung

Ereignis Umwandlung	
Mit Finger Türe öffnen	Keine Umwandlung
Mit Finger Türe dauerhaft öffnen	Keine Umwandlung
Mit Finger Türe dauerhaft sperren	Keine Umwandlung
Mit Finger Alarmananlage ein	Keine Umwandlung
Mit Finger Alarmananlage aus	Keine Umwandlung
Anschluß 2 schalten	Keine Umwandlung
Anschluß 3 schalten	Keine Umwandlung
Ablehnung unbekannter Finger	Keine Umwandlung
Ablehnung bekannter Finger	Keine Umwandlung
Mit Finger Türe öffnen (lokales Relais)	Keine Umwandlung

Die Ereignis-Umwandlung ist der wesentlichste Grund, warum man ein neues Gerät überhaupt anlegt. Hier kann definiert werden, dass dieser neu angelegte Typ von Fingerscanner nicht das einem Finger zugeordnete Standard- Ereignis auslöst, sondern eben ein anderes. Damit ist es möglich mit einem Finger auf einem Fingerscanner das Ereignis „Mit Finger Türe öffnen" und auf dem neu konfigurierten Fingerscanner z.B. „Anschluss 2 schalten" auszulösen.
Das klingt kompliziert, ist es aber nicht. Zur Veranschaulichung soll folgendes Beispiel Hilfe bieten.

Nehmen wir an, dass Hr. Max Mustermann eine Tür mit einem Fingerscanner absichern will. Zusätzlich möchte er bei einer anderen Tür und damit einem anderen Fingerscanner mit dem gleichen Finger die Alarmanlage aktivieren. Er möchte für beide Funktionen den rechten Zeigefinger verwenden. Für die Ausführung der Aktionen verwendet er eine ekey net SE Aufputz.
Was möchte Hr. Mustermann machen:
Für das Öffnen der Tür ->**Ereignis** „mit Finger Türe öffnen ->**Aktion**: Impuls Anschluss 1
Für die zusätzliche Aktivierung der Alarmanlage: ->**Ereignis** „Alarmanlage Ein" ->**Aktion**: Anschluss 2 schalten
Wie geht er nun vor?Er nimmt nun seinen rechten Zeigefinger im System auf, weist diesem „**mit Finger Türe öffnen**" zu und setzt die Berechtigungen.
Wann immer er nun bei einem berechtigten Fingerscanner seinen rechten Zeigefinger zieht, so wird das Ereignis „Mit Finger Türe öffnen" ausgelöst und damit ein 3sek. Impuls auf Anschluss 1 ausgelöst.

Er möchte aber dass bei dem Fingerscanner zur Aktivierung der Alarmanlage mit dem rechten Zeigefinger die Alarmanlage scharf schaltet. Also muss er nun ein neues Gerät definieren. Dort definiert er unter Ereignisumwandlung.

Mit Finger Türe öffnen	Anschluss 2 schalten

Der Fingerscanner wandelt das Ereignis „mit Finger Türe öffnen" in Anschluss 2 schalten".

Sie können hier nun für den neuen Fingerscanner, die den Fingern zugeordneten Ereignisse entsprechend wandeln.

8.1.4.1.4 Einstellungen für neue Typen ekey net 3 SE AP



8.1.4.1.4.1 Geräteanschlüsse

Bezeichnung Anschluss 1:

Bezeichnung Anschluß 1	Relais 1

Hier wird die Bezeichnung des Relais 1 (CHANNEL1) der ekey net SE AP definiert. Als Standard wird dieses mit "Relais 1" definiert. Sie können aber jede beliebige Bezeichnung verwenden.

Bezeichnung Anschluss 2:

Bezeichnung Anschluß 2	Relais 2

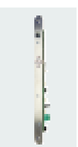
Hier wird die Bezeichnung des Relais 2 (CHANNEL2) der ekey net SE AP definiert. Als Standard wird dieses mit "Relais 2" definiert. Sie können aber jede beliebige Bezeichnung verwenden.

Bezeichnung Anschluss 3:

Bezeichnung Anschluß 3	Relais 3

Hier wird die Bezeichnung des Relais 3 (CHANNEL3) der ekey net SE AP definiert. Als Standard wird dieses mit "Relais 3" definiert. Sie können aber jede beliebige Bezeichnung verwenden.

8.1.4.1.5 Einstellungen für neue Typen ekey net 2 SEIN



8.1.4.1.5.1 Geräteanschlüsse

Bezeichnung Anschluss 1:

Bezeichnung Anschluß 1	Relais 1

Hier wird die Bezeichnung des Relais 1 (CHANNEL1) der ekey net SE IN definiert. Als Standard wird dieses mit "Relais 1" definiert. Sie können aber jede beliebige Bezeichnung verwenden.

Bezeichnung Anschluss 2:

Bezeichnung Anschluß 2	Relais 2

Hier wird die Bezeichnung des Relais 2 (CHANNEL2) der ekey net SE IN definiert. Als Standard wird dieses mit "Relais 2" definiert. Sie können aber jede beliebige Bezeichnung verwenden.

Bezeichnung Anschluss 3:

Bezeichnung Anschluß 3	Taster

Die ekey net SE integra hat einen digitalen Eingang über den z.B. der Türstatus (Tür offen bzw. Tür geschlossen) ins System eingelesen werden kann. Die Bezeichnung für diesen Eingang ist hier zu definieren. Der Zustand des Einganges kann im Gerätestatus abgefragt werden und weiters können Sie, wenn Sie ein Logging aktivieren, Statusänderungen dieses Einganges in den entsprechenden Log-Files protokollieren und dann nachvollziehen.

8.1.4.1.6 Einstellungen für neue Typen ekey net 1SE mini



8.1.4.1.6.1 Geräteanschlüsse

Bezeichnung Anschluss 1:

Bezeichnung Anschluß 1	Relais 1

Hier wird die Bezeichnung des Relais 1 (CHANNEL1) der ekey net SE mini definiert. Als Standard wird dieses mit "Relais 1" definiert. Sie können aber jede beliebige Bezeichnung verwenden.

Bezeichnung Statuseingang 1:

Bezeichnung Statuseingang 1	Türstatus 1

Die ekey net SE Mini hat einen digitalen Eingang über den z.B. der Türstatus (Tür offen bzw. Tür geschlossen) ins System eingelesen werden kann. Die Bezeichnung für diesen Eingang ist hier zu definieren. Der Zustand des Einganges kann im Gerätestatus abgefragt werden und weiters können Sie, wenn Sie ein Logging aktivieren, Statusänderungen dieses Einganges in den entsprechenden Log-Files protokollieren und dann nachvollziehen. Sie wissen dann, wann eine Tür offen war und wieder geschlossen wurde.



Vergeben Sie hier einen sprechenden Namen wie z.B. „Lagertüre 1". Mit dieser Bezeichnung erkennen Sie dann sofort den zugehörigen Logeintrag.

8.1.4.1.7 Einstellungen für neue Typen ekey net CV WIEG



8.1.4.1.7.1 Wiegandoptionen

Der ekey net CV WIEG setzt bei Auftreten eines definierten Ereignisses ein Datenpaket im WIEGAND-Protokoll ab. Grundsätzlich arbeitet der ekey net CV WIEG wie eine Steuereinheit, schaltet aber keine Relais sondern liefert Daten an das fremde Wiegand-System.
Dateneingaben vom Fremdsystem ins ekey net über den ekey net CV WIEG sind nichtmöglich!



Protokoll:

Protokoll	Standard

WIEGAND-Protokolle gibt es in verschiedenen Ausführungen, welche sich in Dateninhalt und Bitlängen unterscheiden.

Standard
- Standard
- Pyramid
- Benutzerdefiniert

Bei der Einstellung „**Standard**" sind alle Dateninhalte und die Bitlängen wie folgt vordefiniert: Das „Standard"-Protokoll ist ident mit dem weit verbreiteten „26-Bit Protokoll".

Gesamt Bitlänge	26
OEM Bitlänge	0
Fingerscanner-ID Bitlänge	8
Benutzer-ID Bitlänge	16
OEM Kennung	0

Auch beim „**Pyramid**"-Protokoll sind der Dateninhalt und die Bitlänge vordefiniert:

Gesamt Bitlänge	39
OEM Bitlänge	0
Fingerscanner-ID Bitlänge	17
Benutzer-ID Bitlänge	20
OEM Kennung	0

Bei der Auswahl „**benutzerdefiniert**" können nun die einzelnen Dateninhalte und die Bitlängen definiert werden.

Gesamt Bitlänge	26
OEM Bitlänge	0
Fingerscanner-ID Bitlänge	8
Benutzer-ID Bitlänge	16
OEM Kennung	0

OEM Bitlänge & OEM Kennung:

OEM Bitlänge	0
OEM Kennung	0

Die Bitlänge der OEM-Kennung und die OEM-Kennung selbst sind hier zu definieren.Die OEM-Kennung kann anzeigen, von welchem Unternehmen der Dateninhalt kommt. So kann man z.B. gleich aus einem Datenpaket erkennen, von welcher Filiale die Daten kommen.

Fingerscanner ID Bitlänge:

Fingerscanner-ID Bitlänge	8

Fingerscanner ID-Bitlänge definiert die Anzahl der Bits welche die Fingerscanner IDenthält. Die Fingerscanner ID-Länge ist bei der Inbetriebnahme eines Fingerscanners in seinen Eigenschaften zu definieren (siehe Kapitel**13.6.3**)



Benutzer ID Bitlänge:

Benutzer-ID Bitlänge	16

Benutzer ID-Bitlänge definiert die Anzahl der Bits, welche die BenutzerID enthält.



Das definierte Protokoll gilt immer für ein Gerät. Ein definiertes Gerät kann nicht gleichzeitig mehrere Protokollformate senden!

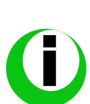
8.1.4.2 Löschen von Gerätetypen

Gerätetypen können, wenn Sie keine Verwendung finden, auch gelöscht werden. ekey empfiehlt dies auch zu tun, da sich die Übersichtlichkeit des Systems verbessert und dadurch die Wartung einfacher und das Risiko von Fehlkonfigurationen minimiert wird.
Wollen Sie ein Gerät löschen, so klickenSieauf das rot „X" neben dem Gerät. Die Löschung erfolgt augenblicklich!



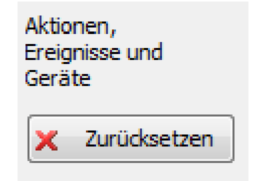


Achten Sie darauf, dass dieser Gerätetyp wirklich nicht mehr verwendet wird. ekey net prüft dies nicht ab und löscht einfach das Gerät!



Sie können kundenspezifische Gerätetypen und keine Standardgerätetypen löschen. Sie erkennen auch den Unterschied zwischen einem Standardgerät und einem kundensspezifischen Gerätetyp, anhand des Löschkreuzes neben dem Gerätetyp!

8.1.4.3 Zurücksetzen von Geräten



Durch Klicken auf den Button "Zurücksetzen" können alle Aktionen, Ereignisse und Geräte auf den Auslieferungszustand zurückgesetzt werden.



ACHTUNG - Alle von Ihnen angelegten und definierten Aktionen, Ereignisse und Geräte werden gelöscht und der Standard lt. Werkseinstellung wiederhergestellt.

8.1.5 Rechte

8.1.5.1 Rechtevergabe an erfasste Administratoren

BUSINESS

LIGHT COM

In diesem Reiter definieren Sie welche Benutzer im ekey net System Administratoren sind, und welche Rechte damit verbunden sind.



Ein Benutzer, dem in diesem Fenster keine Administrationsrechte vergeben werden, kann den ekey net Admin nicht öffnen.



Administrator-Rechte sind völlig unabhängig von den Zutritts-Rechten!!

Administratoren, können, nach Eingabe des persönlichen Passwortes und dem Start des Programms ekey net Admin Einstellungen und Parametrierungen im ekey net System vornehmen.

Administrator | Mustermann, Max

In diesem Kombinationslistenfeld sind die angelegten Administratoren gelistet. Hier ist der Administrator zu wählen, dessen Rechte Sie einsehen bzw. ändern möchten.



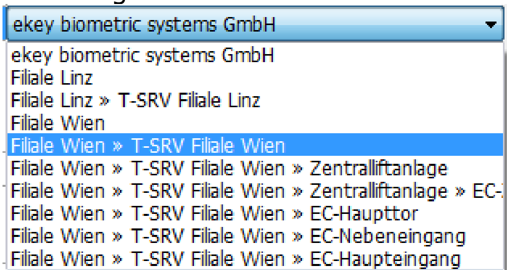
Hier können Sie das Kennwort des Administrators ändern bzw. vergeben.



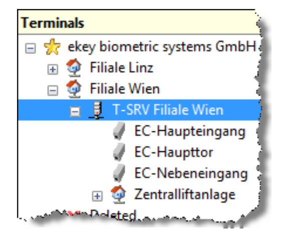
Achtung! Sie sehen das Kennwort nie im Klartext. Vergessen Sie es, haben Sie keine Möglichkeit mehr den ekey net Admin zu starten. Nur ein weiterer Admin könnte dann den ekey net Admin starten und Ihr Passwort neu vergeben!

Verwaltete Terminalgruppe | Terminalgruppen

Hier definieren Sie, auf welche Terminalgruppen der Administrator das Recht besitzt Änderungen vorzunehmen.



Die hier definierbaren Terminalgruppen stimmen natürlich mit der Terminalstruktur überein.



Hier ist auch ersichtlich, dass Sie nur auf 1 Gruppenebene einschränken können.
Im obigen Beispiel sehen Sie, dass „T-SRV Filiale Wien" ausgewählt ist. Damit beziehen sich die Rechte auf die Terminalgruppe „T-SRV Filiale Wien".
Unmöglich ist es bei der obigen Struktur beispielsweise Rechte für „EC-Haupteingang und EC-Nebeneingang" aber nicht für „EC-Haupttor" zu vergeben. Dazu müsste die Terminalstruktur geändert werden.



Berücksichtigen Sie bei der Installation und Anlage der Geräte auch eventuelle Berechtigungseinschränkungen der Administratoren!

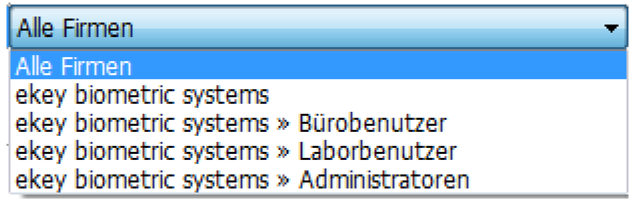
Rechte Terminals	◉ darf bearbeiten ○ darf nur ansehen ○ Portiermodus

Hier definieren Sie welche Rechte der Administrator im gewählten Terminalbereich hat

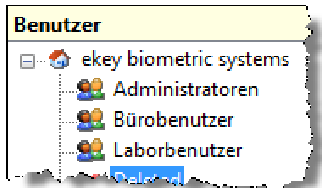
◉ darf bearbeiten	jegliche Bearbeitung ist möglich, Parameteränderungen, Geräteanlage ,….
◉ darf nur ansehen	der Administrator darf nur die Terminalstruktur einsehen, aber keine Änderungen vornehmen
◉ Portiermodus	Portiermodus (siehe Kapitel9)

Verwaltete Benutzergruppe	Alle Firmen

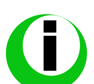
Hier definieren Sie in welcher Usergruppe der Administrator das Recht besitzt Änderungen vorzunehmen.



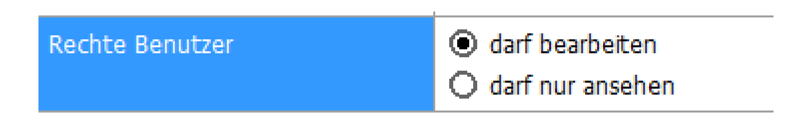
Die hier verwaltbaren Benutzergruppen stimmen natürlich mit der Benutzerstruktur überein.



Analog zu den Terminalrechten können Sie auch hier nur auf 1 Usergruppenebene Rechte vergeben.



Berücksichtigen Sie bei der Benutzeranlege auch eventuelle Berechtigungseinschränkungen der Administratoren!



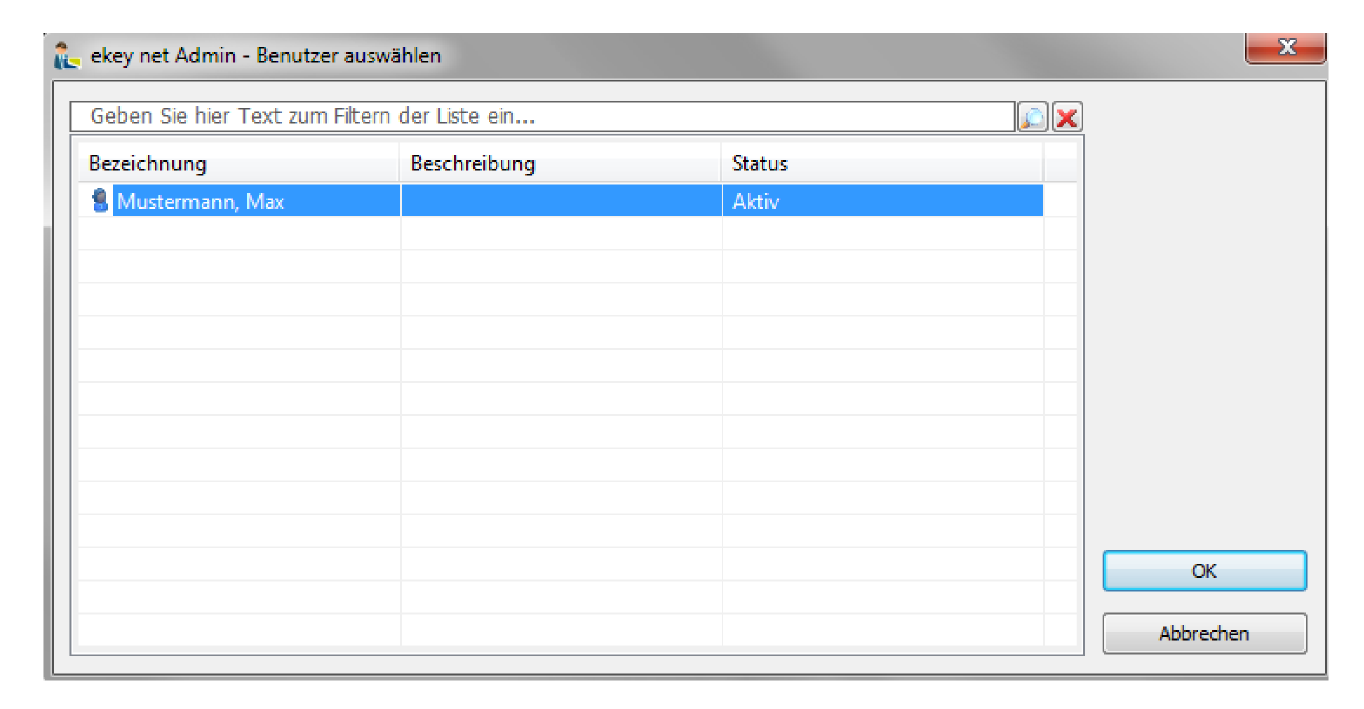
Hier definieren Sie welche Rechte der Administrator in der gewählten Benutzergruppe hat:

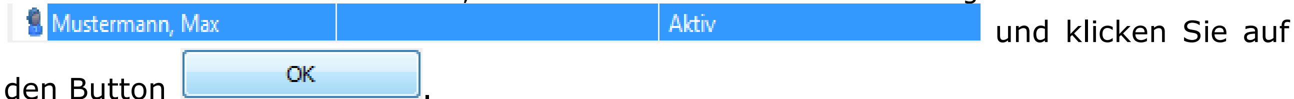
◉ darf bearbeiten	jegliche Bearbeitung ist möglich, wie z.B. Parameteränderungen,Geräteanlage ,….
◉ darf nur ansehen	der Administrator darf nur die Terminalstruktur einsehen, aber keine Änderungen vornehmen

8.1.5.2 Neue Administratoren anlegen

Um einen neuen Administrator anzulegen, klicken Sie auf der rechten Seite auf 

Es öffnet sich eine Liste mit allen im System vorhandenen Benutzern. Die Liste ist alphabetisch nach Nachnamen sortiert. Im Feld über der Namensliste haben Sie noch eine Filtermöglichkeit.Falls die Benutzeranzahl sehr groß ist, können Sie hier die Liste einschränken.



Wählen Sie nun hier den Benutzer, welchem Sie Administrationsrechte geben wollen.


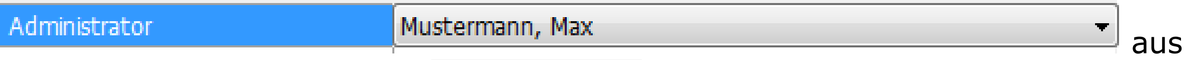
und klicken Sie auf den Button OK.



Achtung! Geben Sie unbedingt ein Kennwort für den neuen Administrator ein!

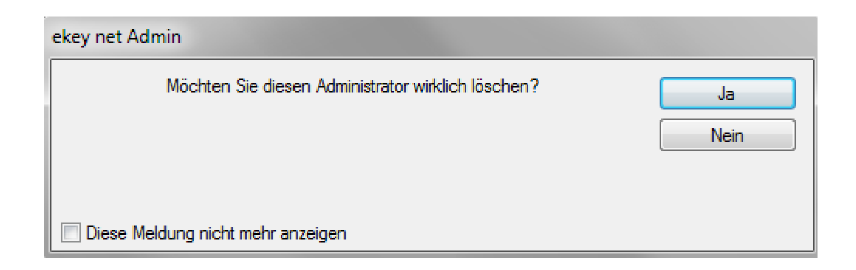
Der Benutzer wird nun in die Liste der Administratoren übernommen. Die weiteren Rechte für diesen Administrator definieren Sie bitte nun lt. Kapitel 8.1.5.1

8.1.5.3 Administrator löschen

Um einen Administrator zu löschen, wählen Sie den gewünschten Administrator im Feld


aus.

Anschließend klicken Sie auf Löschen. Folgend erscheint ein POP-Up Fenster mit folgendem Inhalt:



Klicken Sie hier auf Ja, wird der Administrator gelöscht.



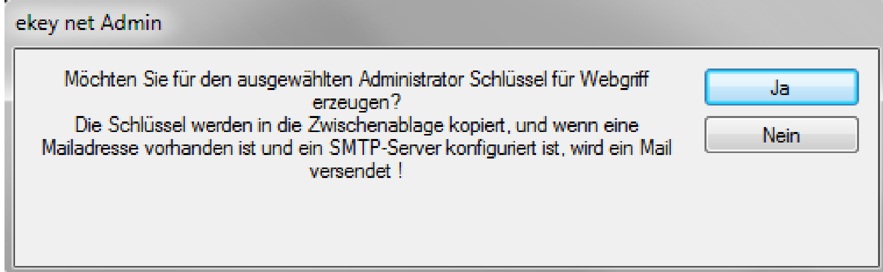
Löschen Sie hier einen Administrator, so wird er nur aus der Administratorenliste entfernt und seine Administrationsrechte werden gelöscht. Die Zutrittsrechte bleiben uneingeschränkt erhalten!!

8.1.5.4 Schlüsselvergabe für Web-Zugriff

Administratoren können ekey net auch über WEB-Zugriff steuern. Um dieser Möglichkeit der Fernsteuerung von ekey net auch die notwendige Sicherheit gegen unerlaubten Zugriff zu geben, können hier Schlüssel für den Zugriff erstellt werden.

Klicken Sie für die Erzeugung von Schlüssel für den ausgewählten Administrator auf den Button Neue Schlüssel.

Es erscheint folgendes Fenster:



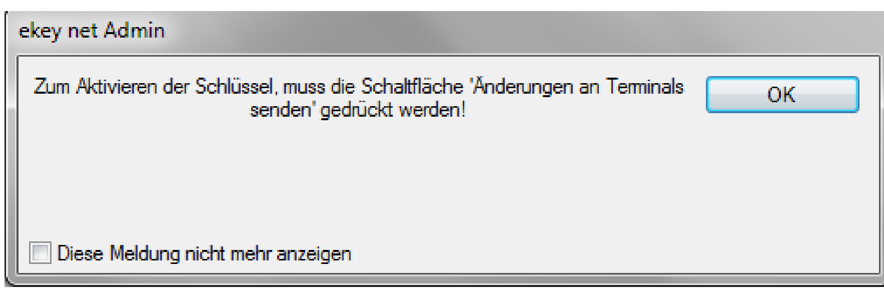
Klicken Sie auf den Buttonum die Schlüssel zu erzeugen.
Der Schlüssel wird entweder

- In die Windows- Zwischenablage kopiert. Von dort können Sie diese in eine Anwendung kopieren.
- Wenn beim Administrator die Emailadresse eingerichtet ist (+ SMTP Server konfiguriert), werden die Schlüssel an diese Adresse versandt.



Haben Sie Schwierigkeiten beim Versand der Schlüssel über Email, nehmen Sie bitte mit Ihrer IT-Abteilung Kontakt auf ! IT-Spezialisten kennen die notwendigen Einstellungen





Damit der Webzugriff dann aber auch richtig funktioniert, müssen Sie noch die Schaltfläche



klicken.

Insgesamt werden 16 Schlüssel in einem Satz mit einer Anforderung vergeben. Jeder Dieser Schlüssel ist einmal verwendbar.

Beispiel für einen Schlüsselsatz:

28-HXVF-POML-IJMS
28-OSPQ-HTBB-PWKF
28-QTVQ-MKKV-VBFB
28-YQPO-KMEQ-RNDJ
28-UUJA-PQTL-YECP
28-GXGZ-RFPS-XKUY
28-KBAI-ZPHE-RNRB
28-ELLM-AIAN-XWFN
28-BQRI-CXTD-YPGO
28-QZIT-QDLD-UUJG
28-UEQO-GVSV-XLRJ
28-DGYX-OWAQ-EKMG
28-ICOV-HSWH-CPZY
28-GBKL-YBAZ-DOHC
28-CVOO-PZWY-TZDV
28-QCML-CHJB-HNJC

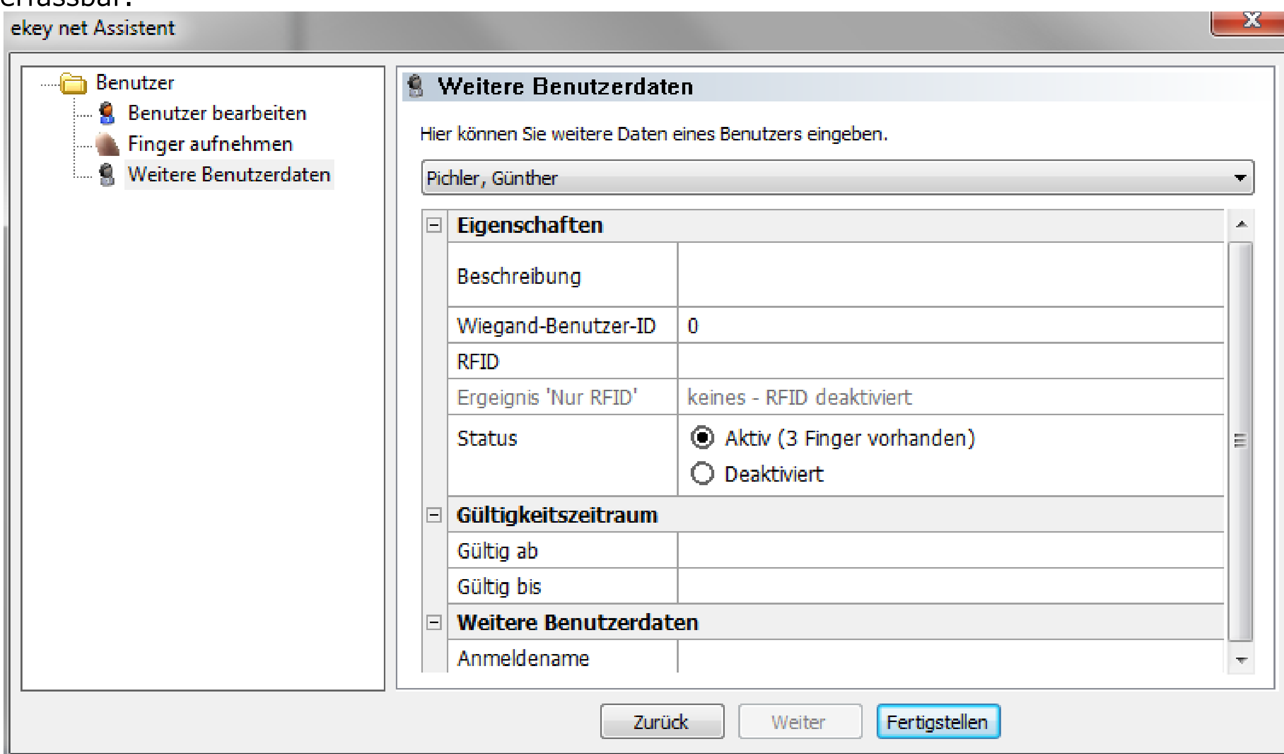
Die Funktion des Web-Zugriffs sehen Sie in Kapitel 11 detailliert beschrieben.

8.1.6 Benutzerdaten



Bei den Lizenzversionen LIGHT und COM gibt es keine zusätzlichen Benutzerdaten!

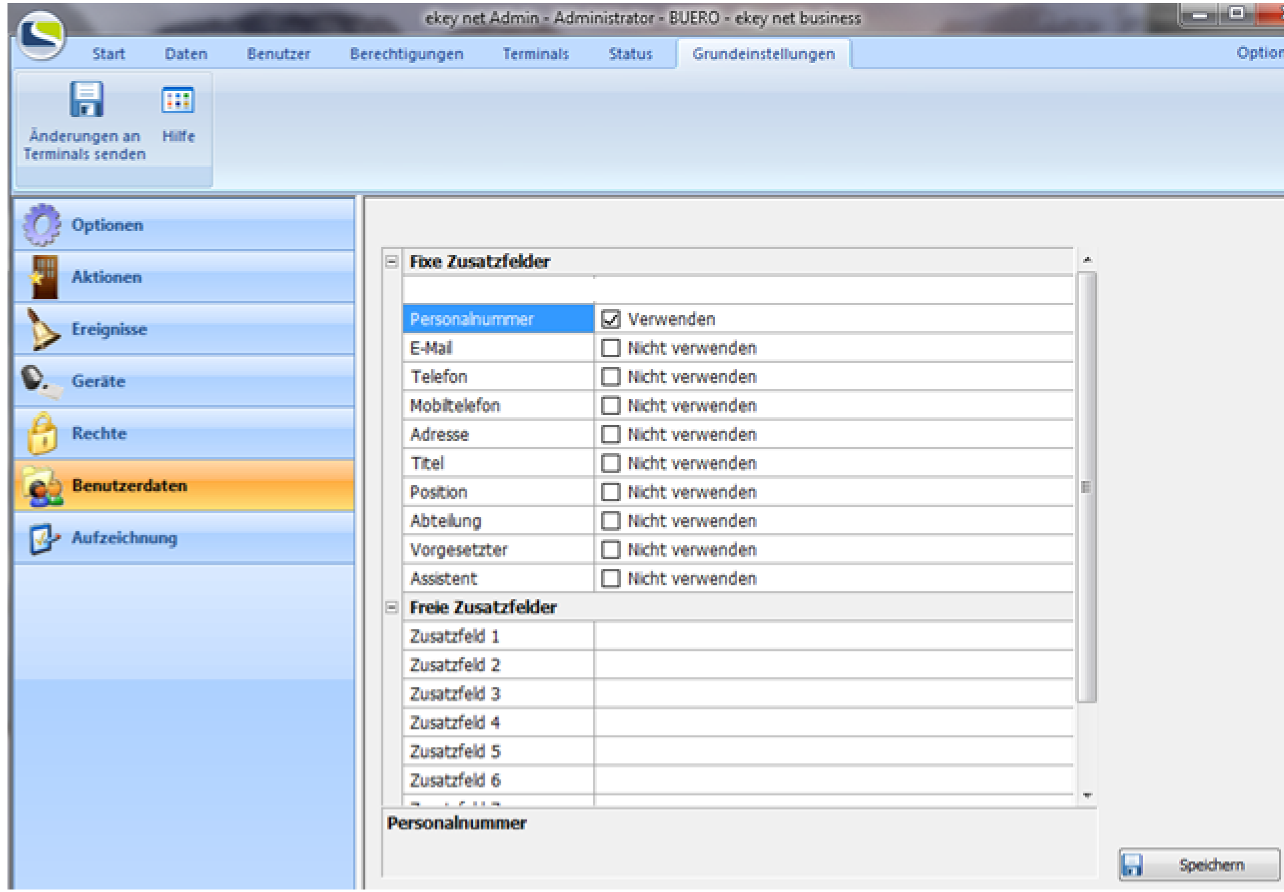
Für jeden Benutzer sind neben seinem Namen und den Fingerdaten noch weitere Daten erfassbar.



In diesem Bereich der Grundeinstellungen können Sie nun weitere Felder definieren die dieser Eigenschaften – Liste der Benutzer hinzugefügt werden. Diese Felder finden Sie dann in den Eigenschaften der Benutzer unter der Rubrik:

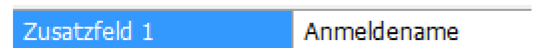






Die Liste der **fixen Zusatzfelder** ist selbstsprechend und es wird nicht weiter darauf eingegangen.

Die Bezeichnungen der 10 **freien Zusatzfelder** können Sie definieren. z.B. Anmeldename, Geschlecht, usw….



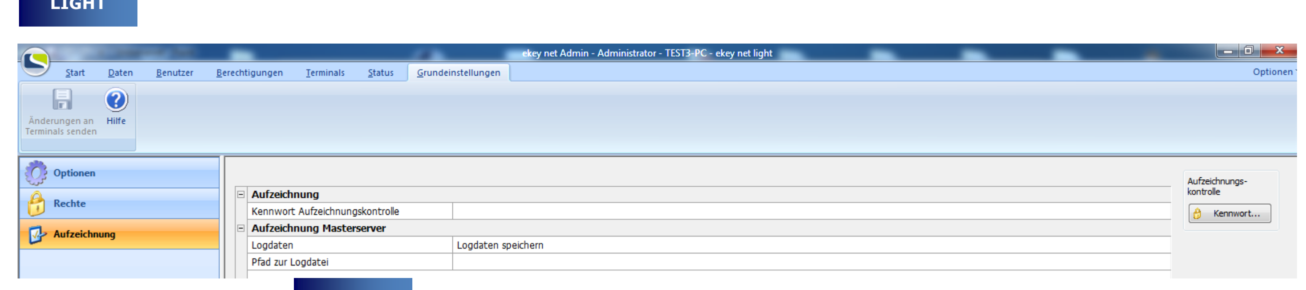
Wird eine Bezeichnung bei einem Zusatzfeld eingetragen, so wird das Feld auch automatisch in den Eigenschaften des Benutzers angezeigt. Sie können dort ihre Eingabe machen.



8.1.7 Aufzeichnung

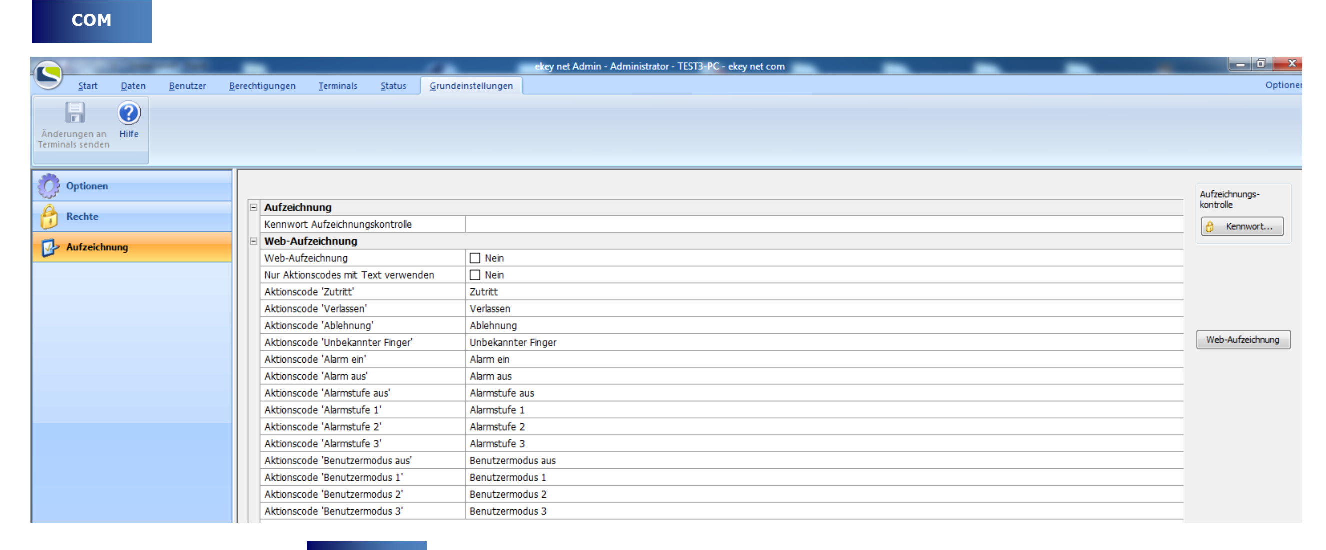
Für Überwachungs- und Protokollierungszwecke des Systems ekey net stehen verschiedene Aufzeichnungsverfahren zur Verfügung. Ob, und welches Aufzeichnungsverfahren Sie verwenden, können Sie in diesem Reiter der Grundeinstellungen definieren.

LIGHT



In der Lizenzversion LIGHT können Sie nur positive Zutritte in eine CSV Datei loggen – Kapitel 15.1.4

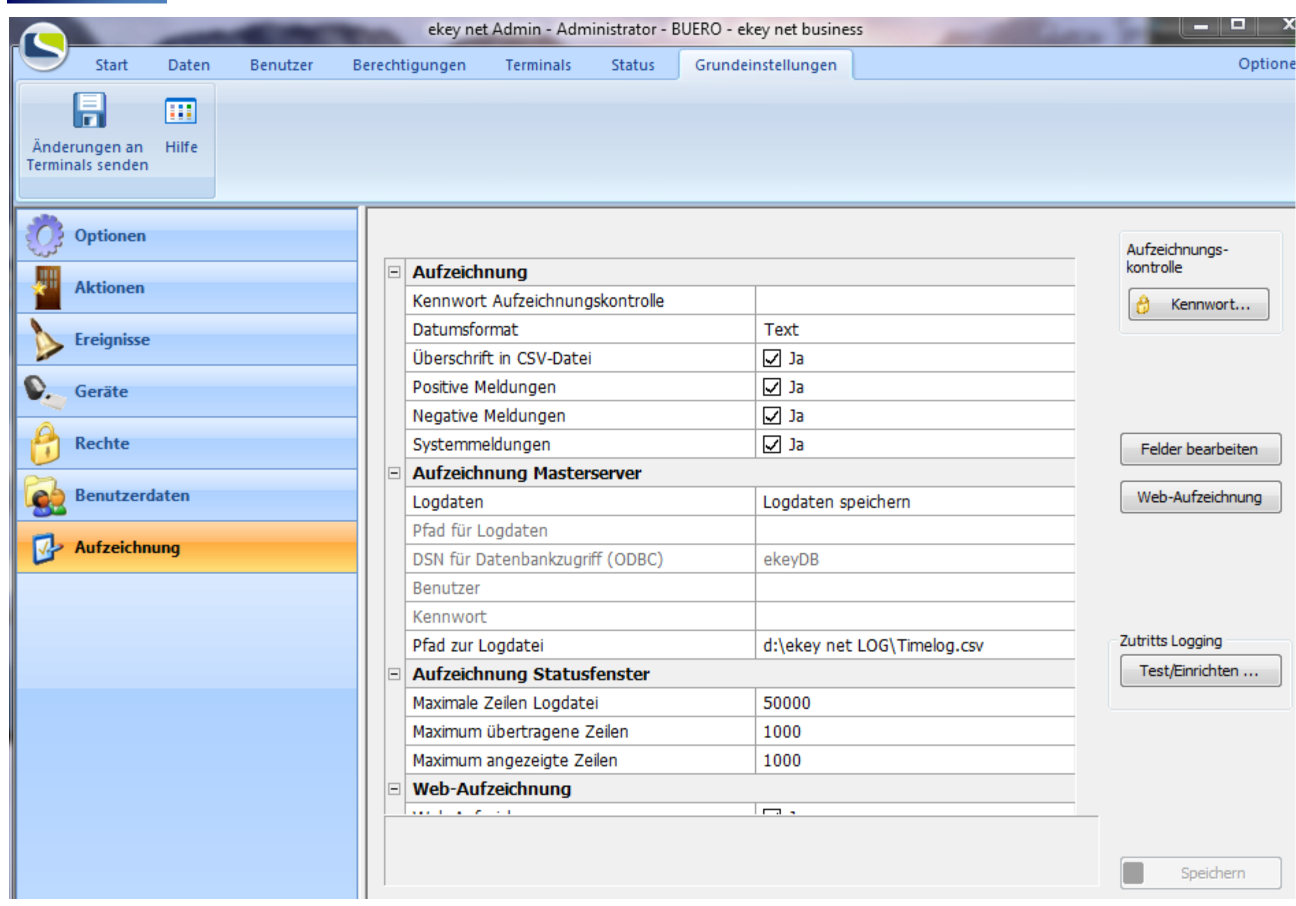
COM



Da in der Version COM vor allem die Kommunikation mit „Etagen – Druckern" das vorrangige Ziel darstellt, können Sie hier alle nötigen Einstellungen für das „Echtzeit – Logging" über das http Protokoll – wir nennen es der Einfach heit halber „Web Aufzeichnung" – durchführen. Details im Kapitel 15.1.7







Die detaillierten Beschreibungen zu allen Aufzeichnungs -Funktionen findenSie im Kapitel 15.1 Aufzeichnung und Speicherung der Daten.

9 Portiermodus

Der Portiermodus von ekey net bezieht sich auf die Funktionalitäteines ekey net Admin. In diesem Modus sind die Rechte der Administration für den entsprechenden Benutzer auf

- Das Öffnen und Schließen von Türen im berechtigten Bereich
- Das Abrufen der Anwesenheitsliste
- Das Abrufen des Gerätestatus im zugewiesenen Bereich

eingeschränkt.

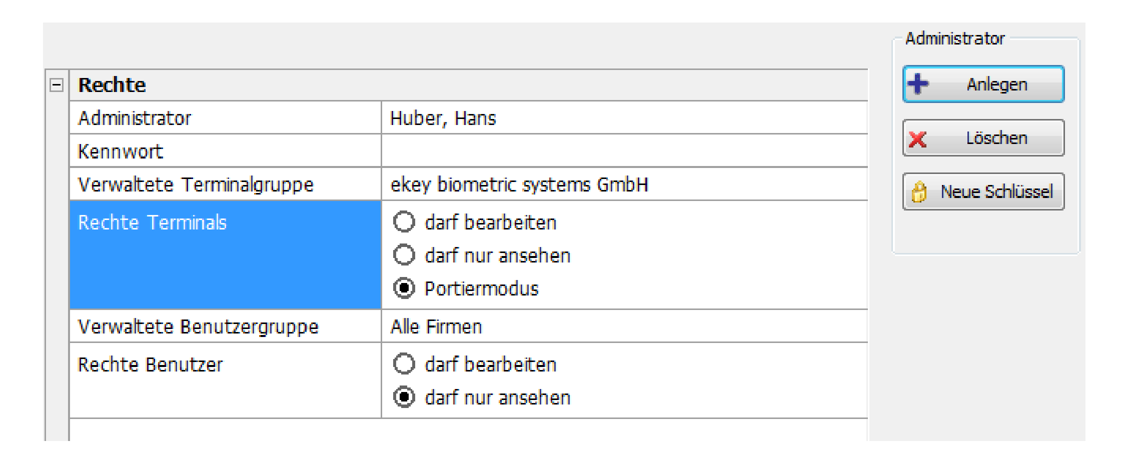


9.1 Aktivierung des Portiermodus

Der Portiermodus des ekey net Admin muss in den „**Grundeinstellungen**" -> „**Rechte**" dem gewünschten Benutzer zugewiesen werden.

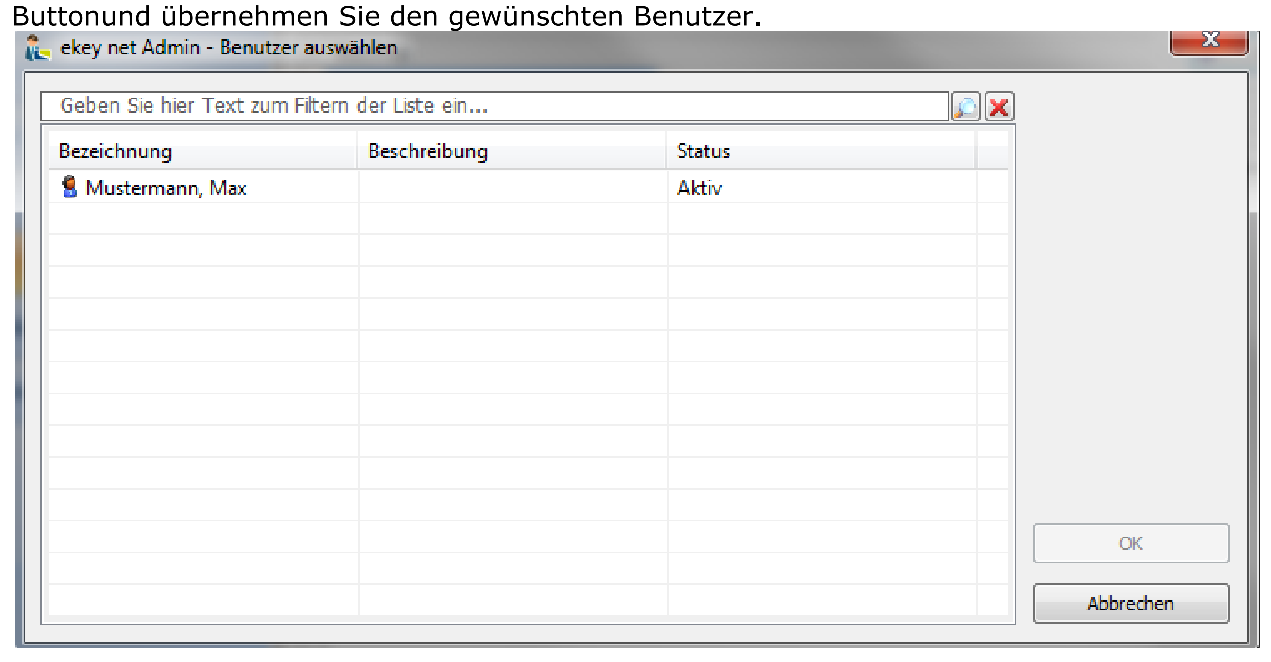


Der Benutzer muss natürlich für die Zuweisung im ekey net bereits bekannt und aktiv sein (Finger eingelesen). Die Eingabe der Benutzerdaten finden Sie im Kapitel 6.4.2.2 erklärt.



Administrator | Huber, Hans

Wählen Sie hier den gewünschten „Portier" aus, in dem Sie die Combobox öffnen.
Ist er in der dabei aufklappenden Liste noch nicht vorhanden,klicken Sie bitte auf den Buttonund übernehmen Sie den gewünschten Benutzer.

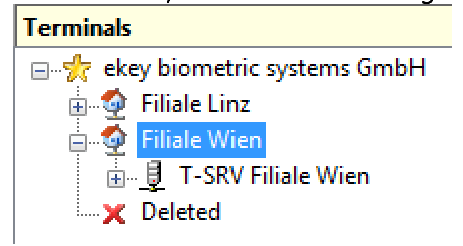


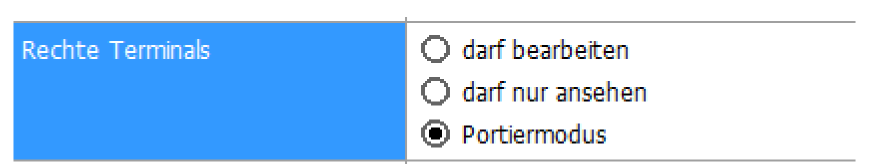
Kennwort | *****

Als nächstes definieren Sie das Kennwort des Portiers.
Das Kennwort ist **„case-sensitiv"** (Achten Sie auf Groß- und Kleinschreibung) und soll mindestens 5 Stellen haben. Die Eingabe von Sonderzeichen ist erlaubt.



Hier definieren Sie, in welchem Terminalbereich der Portier Aktionensetzen bzw. Geräte überwachen darf. In diesem Beispiel sehen Sie die Terminalstruktur einer Anlage mit den 3 Filialen Linz, Wien und Salzburg. Unser Portier soll nur in Wien Zugang erhalten.





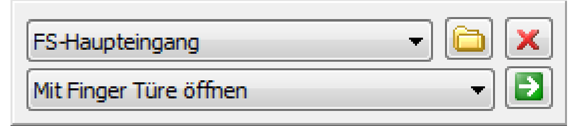
Hier definieren Sie, dass der „Administrator" nur als Portier Zugang zum System erhält, indem Sie die Checkbox ◉ Portiermodus wählen.



Die Auswahl „Portiermodus" führt dazu, dass die Rechte auf Benutzerseite nicht mehr eingetragen werden müssen, da ein Portier keine Benutzerdaten einsehen kann.

9.2 Funktionen im Portiermodus

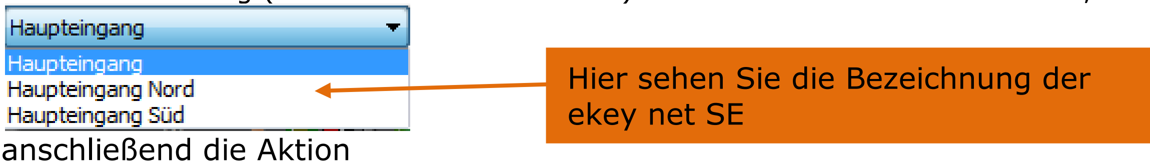
Startet dieser Benutzer den ekey net Admin mit seinem Benutzername und Passwort, so ist automatisch der Portiermodus aktiv und der Admin wird minimiert ausgeführt. Durch Klick aufin der Windows Taskleiste erscheint dann dieses Fenster:



Hier können nun direkt vom PC Schaltaktionen bei den einzelnen konfigurierten ekey net SE ausgeführt werden. Des Weiteren können Sie den Status der Geräte im Bereich abrufen und die Anwesenheitsliste kontrollieren.

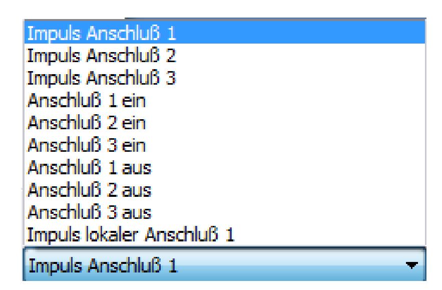
9.2.1 Durchführung von Schaltaktionen

Für eine Schaltung (z.B. zum Öffnen einer Tür) wählen Sie die Steuereinheit aus, und



anschließend die Aktion

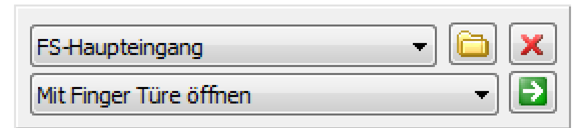




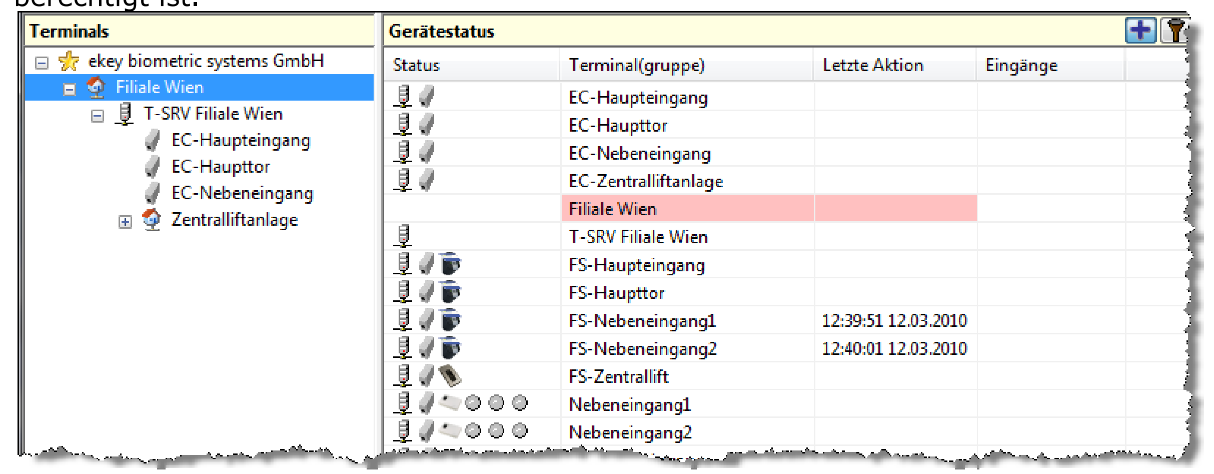
zuletzt klicken Sie auf das Symbol . Damit wird die Aktion an der gewählten ekey net SE ausgeführt. Natürlich werden hier nur die ekey net SE angezeigt, die im Bereich der Berechtigung des Portiers liegen.

Wählen Sie z.B. Steuereinheit **Haupteingang** und **Impuls Anschluss 1,** so schaltet auf der ekey net SE mit der Bezeichnung „Haupteingang" das Relais 1 für 3Sekunden.

9.3 Gerätestatus



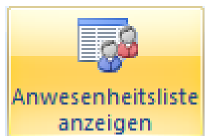
Der Gerätestatus erlaubt ihnen den Zustand der Terminals (Fingerscanner, SE) abzurufen. Klicken Sie dazu auf das Symbol . Der Portier sieht natürlich nur die Geräte, für die er berechtigt ist.



Die detaillierte Beschreibung zum Gerätestatus finden Sie im Kapitel6.7

9.4 Anwesenheitsliste

Die Anwesenheitsliste zeigt ihnen die Anwesenheit der Mitarbeiter im Objekt (Unternehmen). Durch Klick aufund anschließender Auswahl von



startet das Fenster mit der Anwesenheitsliste. Detaillierte Funktionen zur Anwesenheitsliste finden Sie im Kapitel10.



10 Anwesenheitsliste



Für die 100% Vollständigkeit der Anwesenheitsliste (Alle Einträge werden erfasst) ist es unumgänglich, dass Ihr Netzwerk als auch die Rechner /Server auf denen die ekey net Dienste arbeiten, keine Engpässe (Überlastungen) ausweisen. Ekey net kommuniziert mittels eines nicht transportgesicherten Protokolls (UDP) auf Dienstebene. Ist das System überlastet können hier Daten verloren gehen!

10.1 Vorbereitung der Anwesenheitskontrolle

Um die Anwesenheit einer Person im Unternehmen feststellen zu können, muss diese Person auch die Möglichkeit haben das Betreten und das Verlassen des Unternehmens mitzuteilen.

Um dies zu erreichen müssen Sie im ekey net folgende Einstellungen vornehmen:

10.1.1 Verlassen

10.1.1.1 Aktion definieren

Legen Sie im ekey net eine neue Aktion an, deren Aktionscode mit „**Verlassen**" definiert ist.

Aktion bearbeiten	
Beschreibung	Verlassen
Aktionscode	Verlassen
Gerät	Kein Gerät
Schaltmodus	
Selbsthaltung erlauben	☑ Ja
Impulsdauer (ms)	0
LED (einfärbig)	Unverändert
LED (dreifärbig)	Unverändert

10.1.1.2 Ereignis definieren

Definieren Sie ein neues Ereignis und weisen Sie diesem die Aktion lt. 10.1.1.1 zu.

Externes Ereignis bearbeiten	
Beschreibung	Verlassen
Aktion	Verlassen
Zähler	0
Rücksetzen	Nie
Timeout in Sekunden	0
Aktion bei Zählerende	Keine Aktion
Ereigniscode	

10.1.2 Kommen

Das Kommen des Benutzers wird über ein Standardereignisdefiniert. z.B „**mit Finger Türe öffnen**".Hier brauchen Sie also nicht unbedingt weitere Einstellungen vornehmen.



10.1.3 Definition der Erfassungsart

Sie können nun den Zutritt bzw. das Verlassen mit einem Finger erfassen oder auch 2 Finger für die Funktion verwenden.

10.1.3.1 Zutritt / Verlassen mit 2 verschiedenen Fingern

Weisen Sie dem gewünschten Finger des Benutzers ein Ereignis zu dessen Aktion mit dem Aktionscode „Zutritt" definiert ist. z.B. „mit Finger Türe öffnen". Ziehen Sie diesen Finger über den Sensor, so definiert dieser ihre Anwesenheit.

Dem 2. Finger weisen Sie das Ereignis mit der Aktion (Aktionscode) „Verlassen" zu. Dieser Finger definiert dann bei Ziehen über ein berechtigtes Terminal das Verlassen des Gebäudes.

Fingerzuordnung	
Ereignis r. Zeigefinger	Mit Finger Türe öffnen
Wichtigkeit r. Zeigefinger	★★★☆☆
Ereignis r. Mittelfinger	Verlassen
Wichtigkeit r. Mittelfinger	★★★☆☆

In diesem Beispiel machen Sie mit dem
Rechten Zeigefinger -> Anwesenheit
Rechter Mittelfinger -> Abwesenheit



Die Anwesenheit bzw. Abwesenheit können Sie hier an jedem Terminal des Systems ekey netan dem Sie berechtigt sind melden.

10.1.3.2 Zutritt / Verlassen mit 1 Finger

Möchten Sie nur mit einem Finger An-bzw. Abwesenheit melden, so müssen Sie ein gesondertes Terminal (einen eigenen Fingerscanner) montieren und im ekey net eine neue Fingerscannertype erstellen. Sie brauchen also 2 Fingerscanner. In den Eigenschaften der neuen Fingerscannertype definieren Sie nun eine Ereignisumwandlung.

Ereignis bei Ablehnung bekannter Finger	Ablehnung bekannter Finger
Ereignis Umwandlung	
Mit Finger Türe öffnen	Verlassen
Mit Finger Türe dauerhaft öffnen	Keine Umwandlung
Mit Finger Türe dauerhaft sperren	Keine Umwandlung
Mit Finger Alarmananlage ein	Keine Umwandlung
Mit Finger Alarmananlage aus	Keine Umwandlung
Anschluß 2 schalten	Keine Umwandlung
Anschluß 3 schalten	Keine Umwandlung

In unserem Beispiel wird bei diesem Fingerscanner das Ereignis „Mit Finger Türe öffnen" in das Ereignis „Verlassen" gewandelt. Wann immer ein berechtigter Finger über den Sensor gezogen wird, dem das Ereignis „Mit Finger Türe öffnen" zugewiesen ist, wird nicht dieses ausgeführt, sondern das Ereignis „Verlassen".
Damit können Sie mit einem Finger an allen Terminals die Anwesenheit melden, und an der speziellen Fingerscannertype die Abwesenheit, und zwar mit dem gleichen Finger.



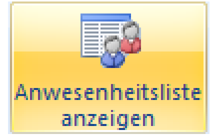
Das Ereignis „Verlassen" kann nur auf den dafür definierten Fingerscannern ausgeführt werden.



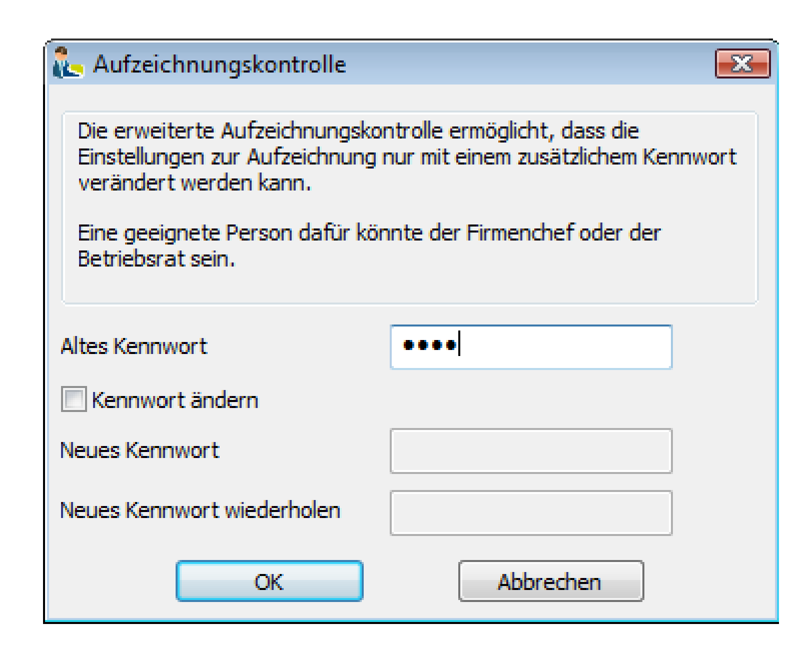
Wenn Sie die Funktion Anwesenheitsliste verwenden, empfehlen wir Ihnen die Variante mit zwei Fingerscannern und einem Finger zu steuern. Die Bedienung des Systems wird damit wesentlich einfacher.

10.2 Arbeiten mit der Anwesenheitsliste

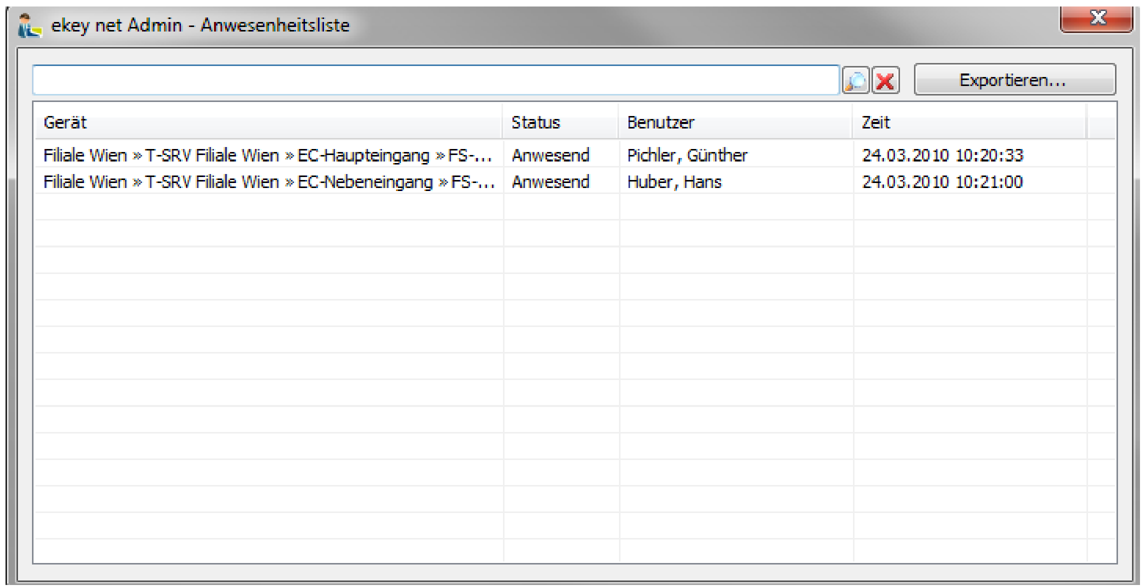
Die Anwesenheitsliste zeigt ihnen die Anwesenheit der Mitarbeiter im Objekt (Unternehmen). Durch Klick auf das Menü **„Daten"** und anschließender Auswahl von



startet das Fenster mit der Anwesenheitsliste. Hier ist nun das Kennwort zur Anzeige der Anwesenheitsliste einzugeben. Das Kennwort ist ident mit dem unter Kapitel 15.1.1 definierten Kennwort. Das Fenster zur Kennworteingabe erscheint nur, wenn Sie auch ein Kennwort definiert haben.



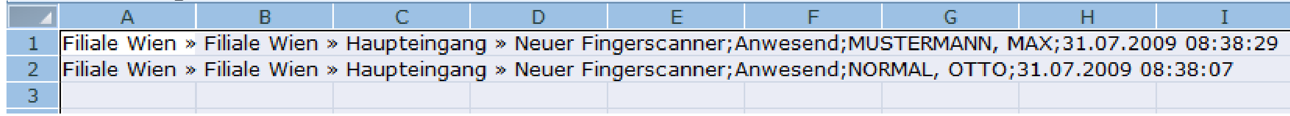
Sie können hier durch Klick auf die Checkboxdas Passwort auch ändern.
Haben Sie das richtige Passwort eingegeben, so startet nun ein Fenster, das ihnen die Anwesenheit der Personen zeigt.



Wen die Liste länger ist können Sie einen Filter setzen (einfach in Textzeile vor dem Symbolden Filterwert eingeben), und so die Liste auswerten bzw. die Anwesenheit von Personen schnell feststellen.

Weiters haben Sie auch die Möglichkeit die Liste zu exportieren. Klicken Sie dazu auf den Button Exportieren… . Es öffnet sich der „Speichern Unter" Dialog von Windows, und Sie können die Liste im .CSV- Format (mit MS-Excel lesbar) mit ihrem gewünschten File-Namen speichern.

In MS-Excel geöffnet sieht die Liste dann z.B. so aus



	A	B	C	D	E	F	G	H	I
1	Filiale Wien » Filiale Wien » Haupteingang » Neuer Fingerscanner;Anwesend;MUSTERMANN, MAX;31.07.2009 08:38:29								
2	Filiale Wien » Filiale Wien » Haupteingang » Neuer Fingerscanner;Anwesend;NORMAL, OTTO;31.07.2009 08:38:07								
3									

11 Web-Zugriff(Handy)

Administratoren haben grundsätzlich die Möglichkeit zur "Fernsteuerung" von ekey net über Web-Zugriff. Administratoren können also aus dem WWW über einen Standard-Browser (z.B. Internet-Explorer,…) ekey net steuern und z.B. Türen öffnen oder Türstati abfragen.



Damit Sie über WWWZugriff auf ekey net bekommen, müssen Sie unbedingt mit Ihrer IT-Abteilung Rücksprache halten. Ihr Netzwerk und die Anbindung ans Internet muss den Zugriffüber Port Nummer: **58007,zu den Rechnern auf denen ekey net Terminalserver laufen,** erlauben.

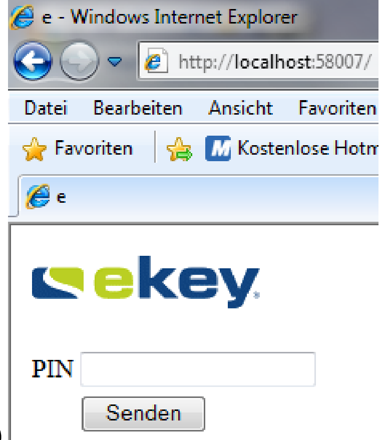
Weiters muss der Benutzer als Administrator im ekey net System bekannt sein!!!

11.1 Verbindung mit PIN (Schlüssel aus ekey net ADMIN)

Wie Sie zu diesen **Schlüsseln** kommen sehen Sie im Kapitel 8.1.5.4

Möchten Sie nun von extern über WWW steuern, so starten Sie dort ihren Browser (z.B. Internet Explorer,…) und geben folgende Zeile im Adressfeld ein:
http://adresse:58007

- **adresse** = ihre öffentliche IP-Adresse oder ihr Domainname über den Sie den Port 58007 zu ekey net routen.



Beispiel (Internet Explorer)

11.2 Verbindung mit USER-ID und KENNWORT

Bei Verwendung dieser Methode brauchen Sie keine Schlüssel.



Die Verbindung ist unsicherer gegenüber dem Zugriff mit Schlüssel(Kennwort ist MD5-gehasht). USERID und KENNWORT könnten „abgehört" werden.Dann hat jeder Zugriff auf ihr ekey net, solange Sie das KENNWORT bzw. die USERID nicht ändern!

Möchten Sie nun von extern über WWW steuern, so starten Sie dort ihren Browser (z.B. Internet Explorer,...) und geben Sie folgende Zeile im Adressfeld ein:
http://adresse:58007/UserID - Aufruf mit UserID und KENNWORT

- adresse = ihre öffentliche IP-Adresse oder ihr Domainname über den Sie den Port 58007 zu ekey net routen.
- Die UserID kann in den Benutzereigenschaften ausgelesen werden. Das KENNWORT ist das zugewiesene Administrator Kennwort aus dem ekey net Admin.

Beispiel (Internet Explorer)

e - Windows Internet Explorer
http://localhost:58007/101
Datei Bearbeiten Ansicht Favoriten E
Favoriten Kostenlose Hotmail
e
ekey
Pwd
Senden

11.3 Temporäre IP-Adressen

Wenn Sie für Ihr Unternehmen (bzw. Ihr Haus) einen Internetzugang ohne fixe IP-Adresse haben, Sie also die IP-Adresse über DHCP von Ihrem Service-Provider zugewiesen bekommen (beispielsweise arbeiten Standard ADSL Zugängen mit Einwahl auf dieser Technologie), so können Sie über die Vielzahl von Dyn-DNS Portalen trotzdemuneingeschränkt, ohne Wissen ihrer derzeitigen zugewiesenen IP-Adresse, Zugang zu ekey net über das WWW erhalten.



Für nähere Informationen sprechen Sie bitte mit ihrem Internet-Service-Provider oder informieren Sie sich z.B. auf www.dyndns.com.

11.4 Sonstige Informationen zum Webzugriff

- Eine Sessionwird nach 60 Sekunden Leerlauf von ekey net geschlossen.

Für diese Funktion muss der Computer, welcher den ekeynet Terminalserverdienst ausführt, über Port 58007 von extern (z.B. aus dem Internet) erreichbar sein.



12 ekey net verbund SE

12.1 Technische Dokumentation

12.1.1 Verkabelung der Komponenten

Mithilfe einer **ekey net Verbundsteuereinheit** kann die Anzahl der schaltbaren Relais auf **max. 28** Relais (7 x ekey net SE REG4) erhöht werden.
Ein Verbund kann nur mit Steuereinheiten erstellt werden, welche den gleichen **ekey net CV LAN** benutzen. Die maximale Geräteanzahl von **8 Geräten pro Bus** gilt auch hierbei (1 Fingerscanner + 7 Steuereinheiten).
Als Basis für den Verbund dienen die Steuereinheiten **ekey net SE mini 1**, **ekey net SE mini 2** oder **ekey net SE REG 4.** Diese werden dann mit den benötigten **ekey net EM mini 3** (Achtung: nur in Verbindung mit einer Steuereinheit verwenden!) oder **ekey net SE REG 4** erweitert.

Beispiel mit ekey net SE mini 2 und ekey net EM mini 3 – Realisierung 20 Relais:

ekey Kabel Typ A
1 gruen
2 gelb
3 braun
4
ekey net SE mini 2
+8-
GND
RELAIS 2
RELAIS 1
ekey net EM mini 3R
RELAIS 5
RELAIS 4
RELAIS 3
RELAIS 8
RELAIS 7
RELAIS 6
RELAIS 11
RELAIS 10
RELAIS 9
RELAIS 14
RELAIS 13
RELAIS 12
RELAIS 17
RELAIS 16
RELAIS 15
RELAIS 20
RELAIS 19
RELAIS 18
ekey net CV LAN
CAT5/CAT6
ekey net

12.1.2 Vorbereitende Konfigurationsschritte

Im ersten Schritt müssen alle ekey net SE, welche später im Verbund zusammengefasst werden, erstellt (konfiguriert werden) – **siehe Kapitel 6.6.3.2.1**



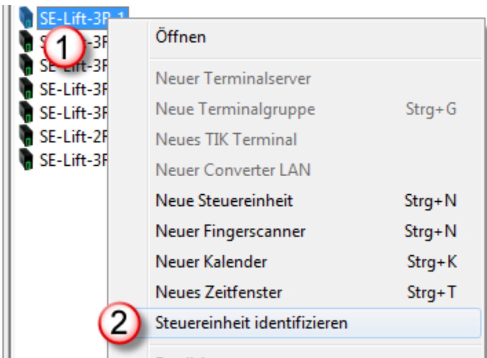
Es empfiehlt sich die ekey net SE mit einer vorläufigen Bezeichnung zu versehen, welche im nächsten Schritt gemäß der tatsächlichen Reihenfolge im Verbund nummeriert wird.

Zur Identifizierung der montierten ekey net SE kann die Funktion **„Steuereinheit identifizieren"** verwendet werden:

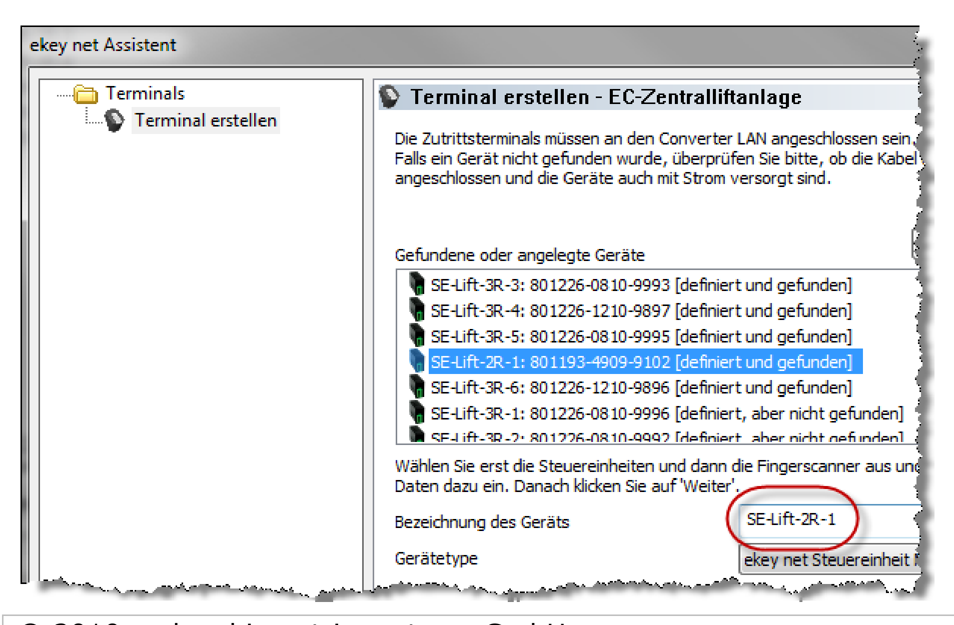
1. Klicken Sie im Übersichtsfenster die entsprechende Steuereinheit mit der recheten Maustaste.

2. Wählen Sie nun im Kontextmenü „Steuereinheit identifizieren"





Das 1. Relais der gewählten ekey net SE schaltet und Sie können so dietatsächliche Position im Verbund bestimmen.Öffnen Sie nun die gewählte Steuereinheit mit der Schaltfläche „Objekt öffnen" oder durch einen Doppelklick und konfigurieren Sie die endgültige Bezeichnung mit der tatsächlichen Positionsnummer.





13 ekey net CV WIEG (WIEGAND Schnittstelle)

ekey net CV WIEG dient zur datentechnischen Ankopplung des Systems ekey net 4.0 an ein externes „Wiegand"-System. Der Datenverkehr passiert dabei unidirektional von ekey net zum Fremdsystem „Wiegand" und niemals umgekehrt.

13.1 Funktionen

Senden von Zutrittsinformationen sofort nach einem Zutritt von ekey net zum Fremdsystem
Zutrittsinformationen: Wiegand_ID

13.2 Eigenschaften

- Der ekey net CVWIEG ist ausschließlich in Verbindung mit ekey net ab Version 3.3 betreibbar.
- Wiegand Protokolle:
  - 26bit - Wiegand
  - Pyramid - Protokoll
  - User defined Protokoll

13.3 Optische Signalisierung am ekey net CV WIEG

Anzeige	Info	Beschreibung
	Grün blinkend	Normalbetrieb
	Grün leuchtend	Daten werden gesendet
	Orange/ rot abwechselnd blinkend	Firmwareupdate
	Orange blinkend	Verbindung zu ekey net CV LAN unterbrochen
	Rot leuchtend	Fehler: z.B. NU

13.4 Verkabelung ekey net CV WIEG

ekey net FS

1 2 3 4 5

NETZANSCHLUSS MIT NETZADAPTER

WIEGAND SYSTEM

10 9 8 7 6 5

1 2 3 4

ekey net CV WIEG

1 2 3 4

ekey net CV LAN

RJ45

ekey net
LAN – Netzwerk
(Ethernet)

* optional

2K2 Resistor

2K2 Resistor

12V

D1

D0

GND

M1 Wiegand Input

D1

D0

GND

ekey

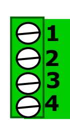
Wiegand Converter

**Beide Widerstände werden nur für Geräte der Fimen NESS und ELK benötigt. Werden NESS / ELK Gerät + Wiegand RFID Leser betrieben, sind diese auch NICHT nötig*

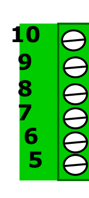


Der ekey net CV WIEG *arbeitet nicht über Bereichsgrenzen hinweg. Aus diesem Grund müssen ekey net FS und der zugeordnete* ekey net CV WIEG *im gleichen RS485 Netz liegen. Beide Geräte müssen somit zum gleichen ekey net CV LAN verbunden werden.*

13.5 PIN- Belegung ekey net CV WIEG



PIN Nr.	ekey net CV WIEG
1	RS485B (KL1)
2	RS485A (KL2)
3	-VCC (KL3) geschalten
4	+ VCC (KL4)



PIN Nr.	ekey net CV WIEG
5	WIEGAND D0
6	WIEGAND D1
7	GND
8	LED 1 (keine Verwendung)
9	- VCC
10	+VCC

Die Spannungsgrenzen (Maximum Ratings) sind entsprechend einzuhalten. Das eingesetzte Gerät mit dem niedrigsten Spannungsbereich definiert die Spannungsgrenzen der Versorgung. Die einzelne Versorgung aller Komponenten ist natürlich auch möglich.

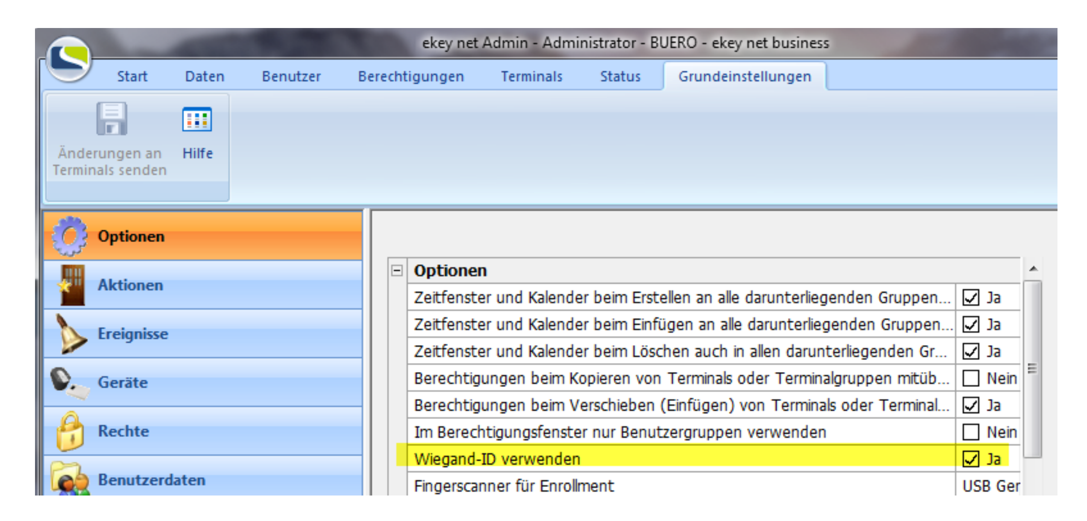


13.6 Aktivierung Wiegand und Zuweisung Wiegand-ID im ekeynet

Die Konfiguration des ekey net CV WIEG erfolgt in der Software ekey net ab Version 3.3.

13.6.1 WIEGAND- Funktion im ekey net aktivieren

Zur Konfiguration der Wiegand-Funktionen im ekey net benötigen Sie uneingeschränkte Administratorrechte. Starten Sie den ekey net Admin und aktivieren Sie unter **„Grundeinstellungen"** -> **„Optionen"** -> das Feld **„Wiegand ID verwenden"**



Damit ist nun die Wiegand-Funktion im ekey net aktiviert. Als nächstes müssen Sie das zu verwendende Wiegand-Protokoll definieren.

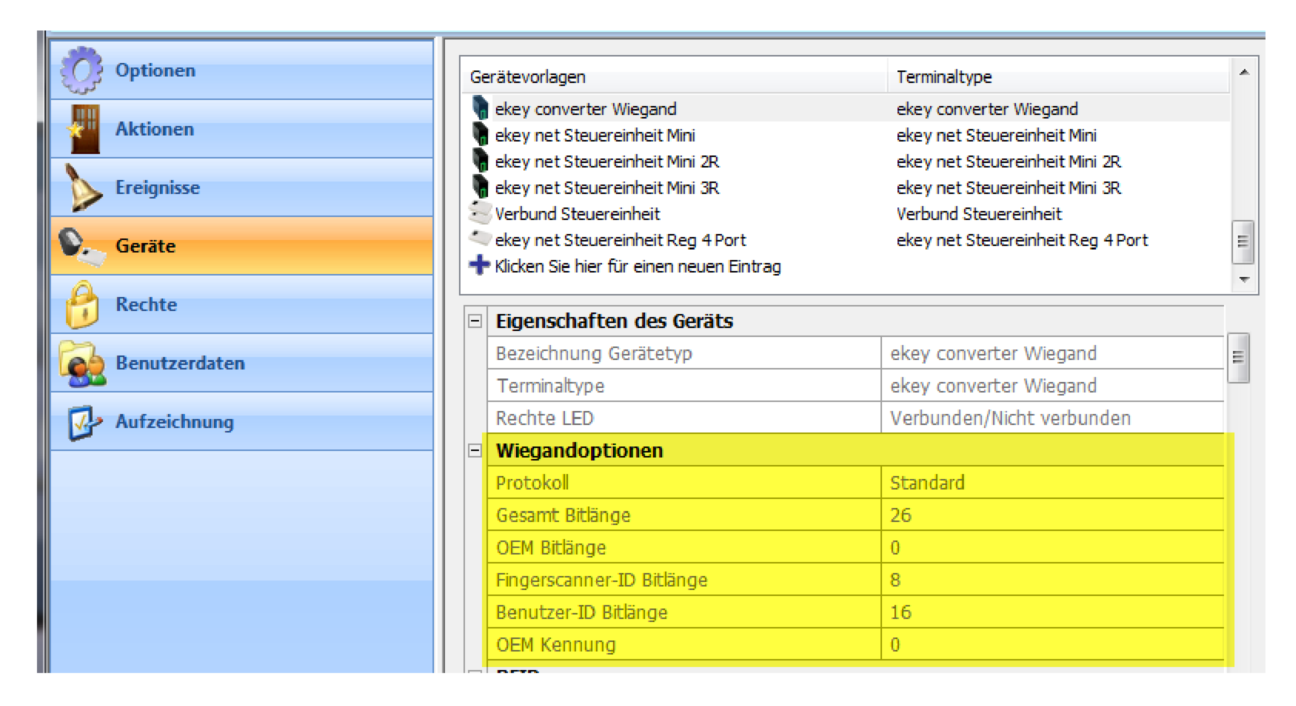
13.6.2 WIEGAND-Protokoll definieren

Wiegand ist von der Protokolldefinition sehr offen und erlaubt die Übertragung benutzer-spezifischer Datenpakete. ekey net hat auf diese Offenheit Rücksicht genommen und Sie können die ID-Bitlängen und die Gesamtlänge pro Terminal frei definieren.

Unter **„Grundeinstellungen"** ->**„Geräte**" -> finden Sie den ekey net CV WIEG
In den Gerätevorlagen finden Sie nun einen vordefinierten ekey net CV WIEGmit dem **Standard** 26bit-Protokoll.

- Gesamtlänge = 26 (inklusive Start & Stopbit)
- Fingerscanner ID- Bitlänge = 8
- Benutzer- ID Bitlänge = 16

© 2010 – ekey biometric systems GmbH



Kann ihr WIEGAND-System nicht mit diesem vordefinierten Gerät arbeiten, weil ihr System andere Bitlängen benötigt, dann können Sie über„**Klicken Sie hier für einen neuen Eintrag**“ ihren spezifischen ekey net CV WIEGdefinieren.

Dabei haben Sie neben dem 26bit-Standardprotokoll zwei weitere Möglichkeiten der Protokolldefinition(klicken Sie dazu ins Eingabefeld „**Protokoll**“ unter „**Wiegandoptionen**“):

- **Pyramid**: 39 bit-Protokoll
- **Benutzerdefiniert**: hier können Sie überhaupt alle ID-Bitlängen frei definieren.

Gesamt-Bitlänge
Entspricht der addierten Bitanzahl von OEM-ID, Fingerscanner-ID und Benutzer ID plus 2 (Start- + Stopbit)

OEM-ID-Bitlänge
Ist die Bitlänge der OEM-Kennung (= Firmen_ID). Die OEM-Kennung wird für den Aufbau organisationsübergreifender Systeme verwendet.Man unterscheidet über diese ID von welchem Unternehmen (Organisation) ein Wiegand-Paket kommt.

Fingerscanner ID-Länge (Geräte ID)
Die Fingerscanner ID-Länge entspricht der Geräte-ID und ist bei den Eigenschaften des zugewiesenen Fingerscanners einzugeben.

Benutzer-ID-Länge
Ist die Bitanzahl der Benutzer-ID, die beim Benutzer eingegeben wird.

13.6.3 Eingabe der einzelnen ID



- Die Eingabe der ID erfolgt als Dezimalwert.
- **Überschreitet** der in den Binärwert umgewandelte Dezimalwert die vorgesehene Bitlänge, so werden die überschreitenden Bits auf MSB-Seite abgeschnitten.

Beispiel 1: (Richtige Eingabe)
z.B.USER ID = 130, FINGERSCANNER ID = 98
Standard-Protokoll 26 bit: Fingerscanner ID Bitlänge = 8
BenutzerID Bitlänge =16
Fingerscanner ID Bit 2 = MSB
Benutzer ID Bit 10 = MSB
PE…. Even parity über Bit 2-13
PO … Odd parity über Bit 14-25

Gesendeter Bitstream an Wiegand-System:

ID	PE	FINGERSCANNER ID								BENUTZER ID																PO
BitNr	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	20	22	23	24	25	26
Inhalt	1	0	1	1	0	0	0	1	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1	0	1

Beispiel 2 (Falscheingabe)



ACHTUNG ! Hier wird dann eine Falsche ID gesandt !!!*ekey net prüft die eingegebene ID nicht gegen die Bitlänge ab.*

Benutzer ID-137 Fingerscanner ID = 276
Standard-Protokoll 26 bit:
Fingerscanner ID Bitlänge = 8
BenutzerID Bitlänge =16
Fingerscanner ID Bit 2 = MSB
Benutzer ID Bit 10 = MSB
PE…. Even parity über Bit 2-13
PO … Odd parity über Bit 14-25

Gesendeter Bitstream an Wiegand

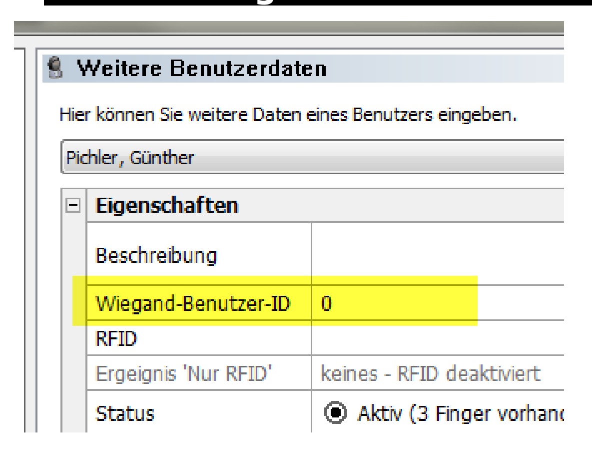
ID	PE	FINGERSCANNER ID								BENUTZER ID																PO
BitNr	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	20	22	23	24	25	26
Inhalt	1	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1	0	0	1	0

Bei der Fingerscanner ID wird das oberste Bit von 276 = 1 0001 0100 abgeschnitten und nur 20 als ID gesandt !!!

Bei der ID-Eingabe ist also unbedingt die Bitlänge zu berücksichtigen. ekey net prüft dies nicht !!

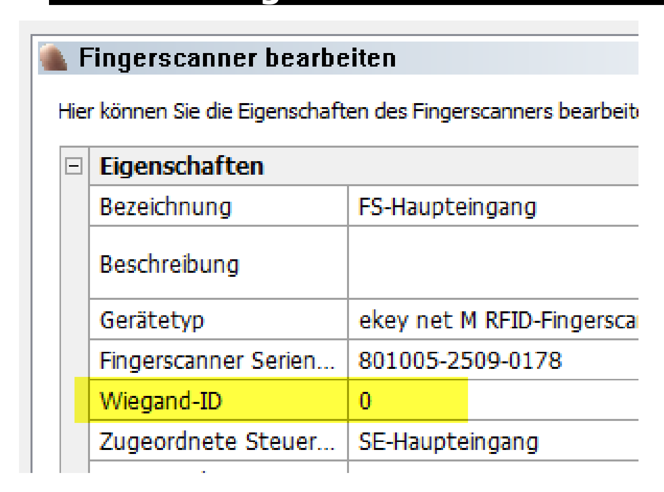


13.6.4 Eingabe Benutzer-ID



Unter „**Benutzer**" ist der entsprechende zu erfassende Benutzer auszuwählen und unter „**Weitere Benutzerdaten**" die „**Wiegand Benutzer ID**" als Dezimalwert einzugeben.
Bitlänge beachten !! (siehe „Eingabe der einzelnen ID"). Die Benutzer ID kann z.B. ident mit der Wiegand-Kartennummerdes Fremdsystems sein.

13.6.5 Eingabe FINGERSCANNER-ID



Wählen Sie unter Terminals den Fingerscanner aus, der die Identifikationsdaten an das Wiegand System senden soll. Definieren Sie in „**Fingerscanner bearbeiten**" des Fingerscanners die „**Wiegand ID"** (=Fingerscanner-ID als Dezimalwert) und definieren Sie unter „**Zugeordnete Steuereinheit**" den entsprechenden ekey CV WIEG.
Bitlänge beachten !! (siehe Eingabe der einzelnen ID)

Parity Bits (erstes und letztes Bit des Wiegand Datenpakets) werden automatisch von ekey net berechnet und sind bei der Eingabe der ID's nicht zu berücksichtigen !

© 2010 – ekey biometric systems GmbH



13.7 Technische Daten (maximum ratings)

Allgemeine Daten (MAXIMUM Ratings)

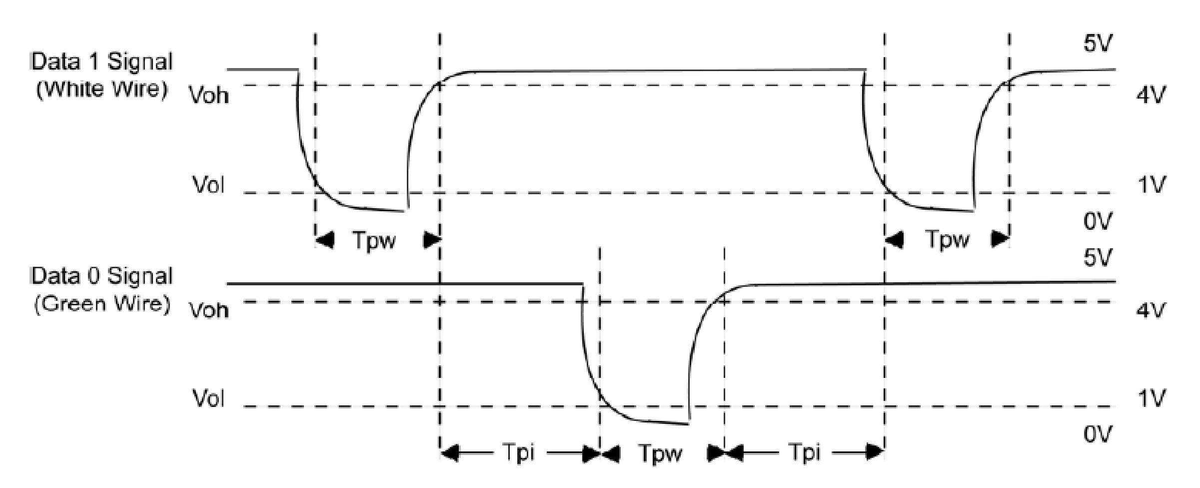
Technische Daten ekey net CV WIEG	Einheit	Werte
Versorgung	VAC	8-24
	VDC	8-30
Leistungsaufnahme	W	ca.1
Temperaturbereich	°C	-20 bis +70
Schutzart		IP20

Spannungsgrenzen D0, D1, LED1 und LED2

D0 und D1 sind Open Collector-Ausgänge. Die entsprechende Last des Mastersystems (Gegenstelle) muß entsprechend angepasst werden.

Wert	Einheit	min	max
VoL (Output Low)	V	4.0	5.5
Voh (Output High)	V	0.0	1.0
Iol (Strom output low)	mA	-1.0	0.0
Ioh (Strom output high)	mA	-25.0	0.0

Signalverlauf auf D0 und D1



Symbol	Beschreibung	Einheit	Zeit		
			min	typ	max
Tpw	Zeit Pulsbreite	µs	20	30	100
Tpi	Zeit Pulsintervall	Ms	1	2	20

14 PowerOn-Reset Sonderkonfiguration

bei starker **E**lectro **S**tatic **D**ischarge - Störung

LAN
Meldung an die ekey net Software

LAN
Schaltbefehl für das WatchDog Relais an die Steuereinheit MINI

Unterbrechung der Stromversorgung 3-4 und Neustart der Geräte

AC/DC IN

Keine Kommunikation auf dem RS 485 BUS

15 Datenlogging

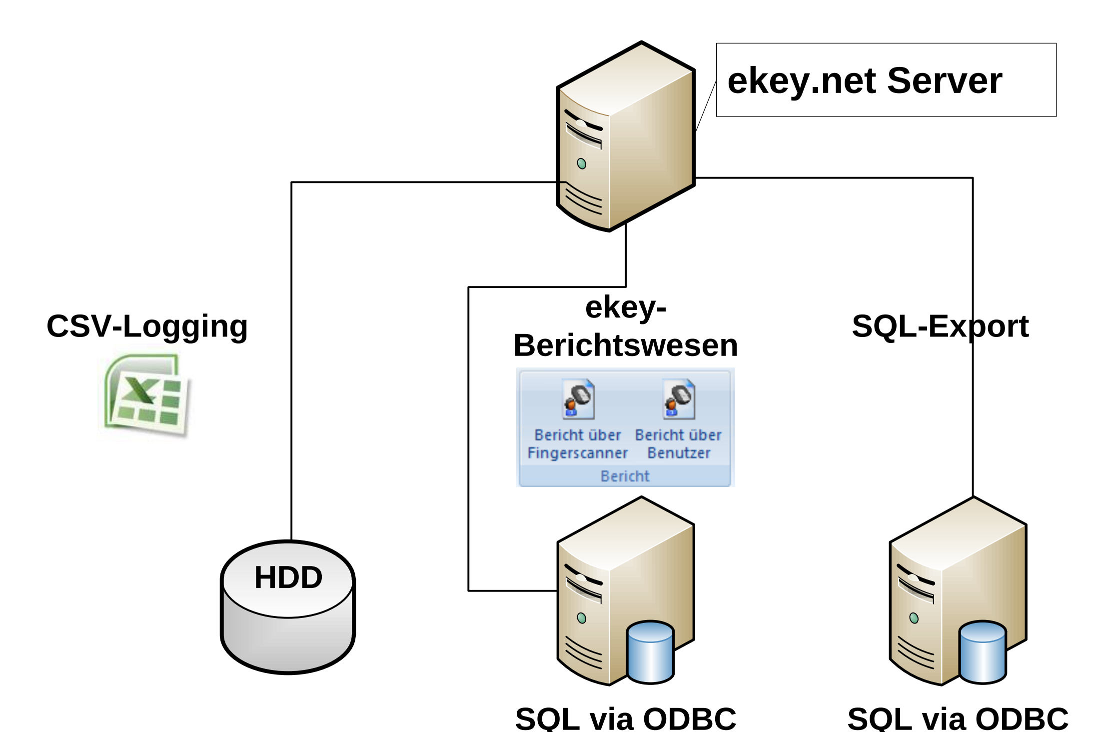


Für die 100%igeVollständigkeit der Log-Daten (alle Einträge werden erfasst) ist es unumgänglich, dass Ihr Netzwerk(Ethernet) als auch die Rechner /Server auf denen die ekey net Dienste arbeiten, keine Engpässe (Überlastungen) ausweisen. Ekey net kommuniziert mittels eines nicht transportgesicherten Protokolls (UDP) auf Dienstebene. Ist das System überlastet können hier Daten verloren gehen!

15.1 Aufzeichnung und Speicherung der Logdaten

ekey net bietet folgende Möglichkeiten Systemdaten (Ereignisse), die während des Betriebs auftreten zu speichern:

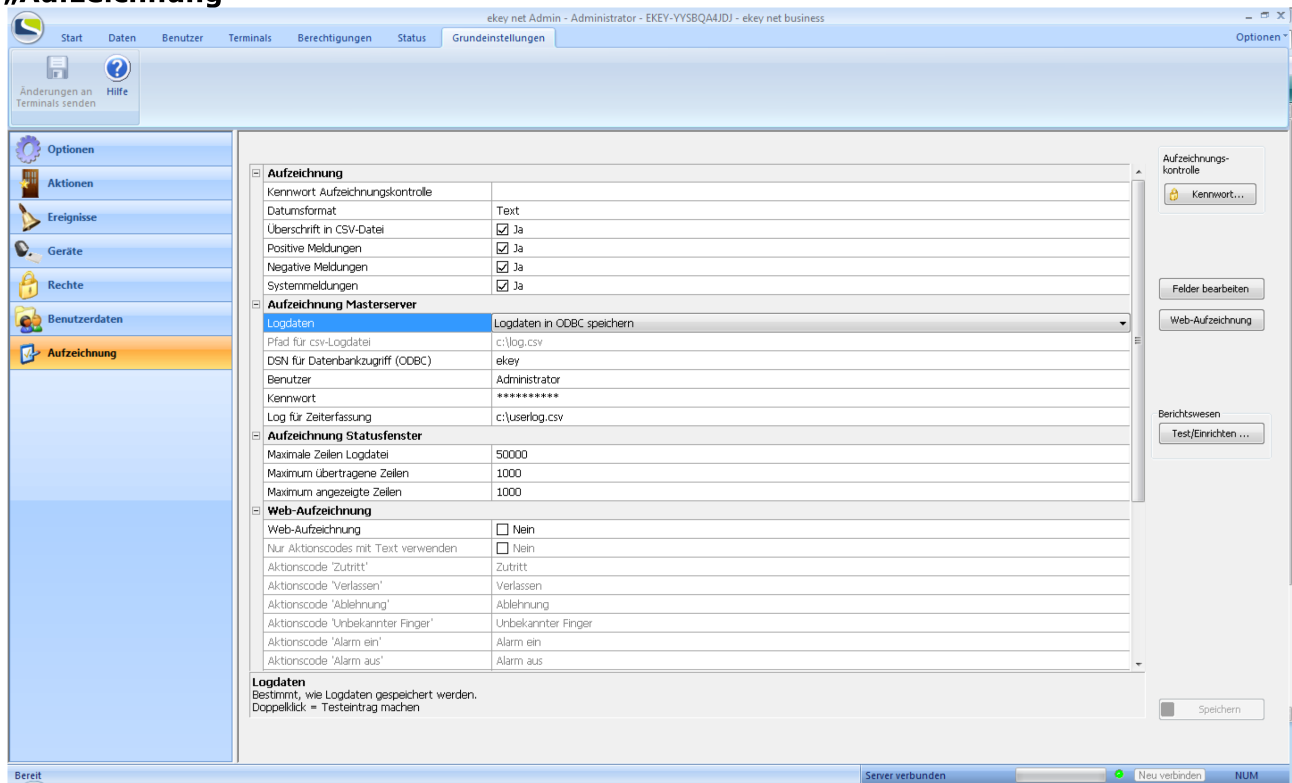
- Logging im CSV-Format (ASCII oder UNICODE)
- ekey-Berichtswesen (SW internes Berichtwesen, setzt ODBC/SQL-Server voraus)
- ODBC/SQL Logging zb. für Anbindung von 3. Softwarelösungen
- WEB-Logging/Ausgabe (Aufzeichnungsausgabe erfolgt mittels html Links zb. für Printserver/Drucklösungen



	CSV-Logging	ekey-Berichtswesen	SQL-Export
	Direktes Speichern auf Lokalen PC oder Netzwerklaufwerk	Am ekey-server muß die ODBC Schnittstelle konfiguriert werden und ein SQL Server installiert werden oder auf einen externen SQL-Server verwiesen werden.	Am ekey-server muß die ODBC Schnittstelle konfiguriert werden und ein SQL Server installiert werden oder auf einen externen SQL-Server verwiesen werden. Sämtliche Tables sind dann dort entsprechend anzulegen.
	Einfache Protokollierung in Tabellenform	Einfaches bequemes Reporting direkt im „ekey-Programm“ 3. Softwareanbieter können die erfassten Daten aus der SQL Datenbank abfragen	3. Softwareanbieter können die erfassten Daten noch detaillierter abfragen und eigene Reports generieren. Die Datenfelder können frei definierbar auch in ein bereits bestehende SQL-Datenbank übergeben werden.
	Installation siehe Punkt 15.1.1.1 „Definition der zu speichernden LOG-Ereignisse“	Installation siehe Punkt 15.1.8 „Berichtswesen (auf SQL Basis)“	Installation siehe Kapitel 15.1.5 „ODBC/SQL Logging“



Die Einstellungen der Logging -Funktionen erfolgt in den Grundeinstellungen unter „Aufzeichnung"



15.1.1 Allgemeine Einstellungen zum Logging

15.1.1.1 Definition der zu speichernden LOG-Ereignisse

Definieren Sie hier welche Ereignisse zu einem Logeintrag führen. Die Einstellungen hier gelten dann für

- CSV- Log Unicode
- CSV – Log ASCII
- ODBC - Log

Aufzeichnung	
Kennwort Aufzeichnungskontrolle	
Datumsformat	Text
Überschrift in CSV-Datei	☑ Ja
Positive Meldungen	☑ Ja
Negative Meldungen	☑ Ja
Systemmeldungen	☑ Ja

Hier können die allgemeinen Einstellungen für das Logging gemacht werden. Die Einstellungen hier gelten dann für alle Arten des Datenloggings.

© 2010 – ekey biometric systems GmbH



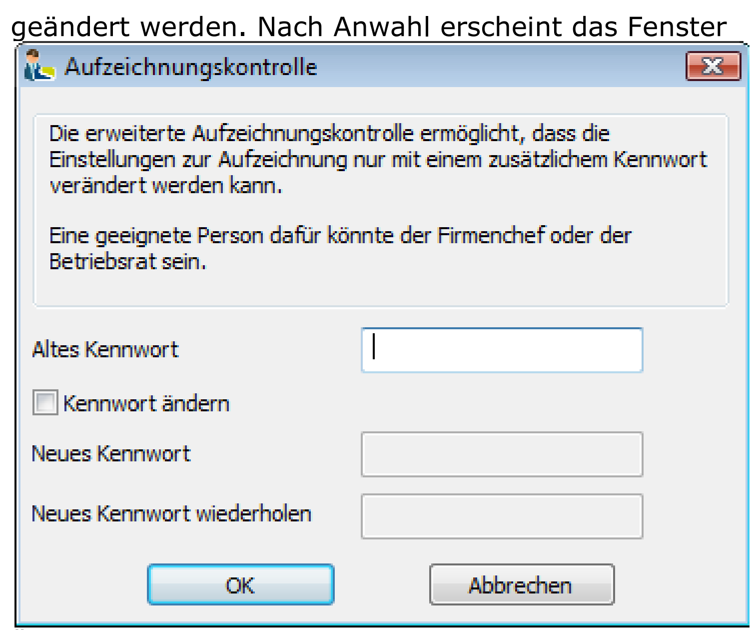
Kennwort Aufzeichnungskontrolle

Haben Sie ein Kennwort für die Aufzeichnungskontrolle vergeben, so müssen Sie dieses hier eintragen, damit Sie Änderungen bei den einzelnen Paramteren der Aufzeichnung vornehmen können.

Das Kennwort kann jederzeit durch Klick auf den Button 

erstellt bzw.

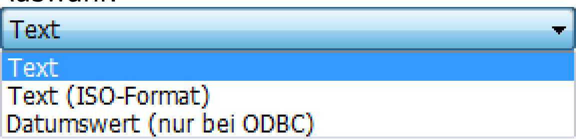
geändert werden. Nach Anwahl erscheint das Fenster



Ändern Sie das Passwort entsprechend der Maskenanweisung. Ab Werk ist kein Kennwort definiert.

Datumsformat	Text

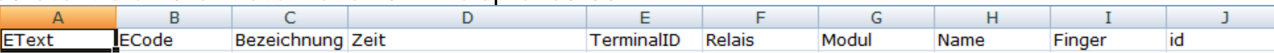
Hier können Sie das Format für Datumseinträge in den Logfiles ändern. Sie haben zur Auswahl:



Die Datumsformate unterscheiden sich wie folgt:
Format „Text“: mm.dd.jjj hh:mm z.B02.07.2009 08:55
Format „Text(ISO-Format)“: jjjj-mm-dd hh:mm:ss.z.B.2009-07-02 13:02:16.00
Datumswert : nur bei ODBC-Logging (nicht bei CSV)
Wählen Sie beim CSV-Logging „Datumswert“, so wird das Datum im „Text(ISO-Format)“ abgespeichert.

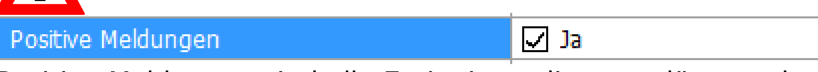
Überschrift in CSV-Datei	☑ Ja

Wählen Sie hier „ja“, so wird in der CSV-Datei die Bezeichnung der einzelnen gewählten Spalten in die ersten Zeile eingetragen.Öffnen Sie mit Hilfe von MS Office Excel die CSV-Datei, so stellt sich die Erste Zeile zum Beispiel so dar:



A	B	C	D	E	F	G	H	I	J
EText	ECode	Bezeichnung	Zeit	TerminalID	Relais	Modul	Name	Finger	id

Sie sehen in Ihrer Anwendung nur die Feldbezeichnungen, die Siegewählt haben !



Positive Meldungen sind alle Ereignisse, die ausgelöst werden

- Durch einen erkannten Finger / Karte
- Der/ die berechtigt zum Zutritt ist (keine Zeitfenstereinschränkung)

Wird ein Finger bzw. eine Karte erkannt aber der Benutzer darf aufgrund einer zeitlichen Einschränkung trotzdem nicht hinein, so ist dies eine negative Meldung.

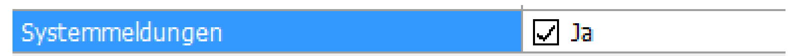
Wählen Sie hier ja, werden alle diese positiven Ereignisse in das Log-File eingetragen



Negative Meldungen sind alle Ereignisse die ausgelöst werden durch

- Ziehen eines unbekannten Fingers oder Vorhalten einer unbekannten RFID-Karte
- Abweisung aufgrund fehlender Berechtigung (Zeit, Kalender)

Wählen Sie hier ob diese Ereignisse in das Logfile mit erfasst werden sollen.



Systemmeldungen sind Ereignisse die das System selbst ausführt, ohne dass Benutzer Eingaben machen (ausgenommen das Anmelden am ekey net Admin) wie z.B.

- Lernfinger
- Admin Logon
- Datenaktualisierung auf Gerät
- verbunden / nicht verbunden

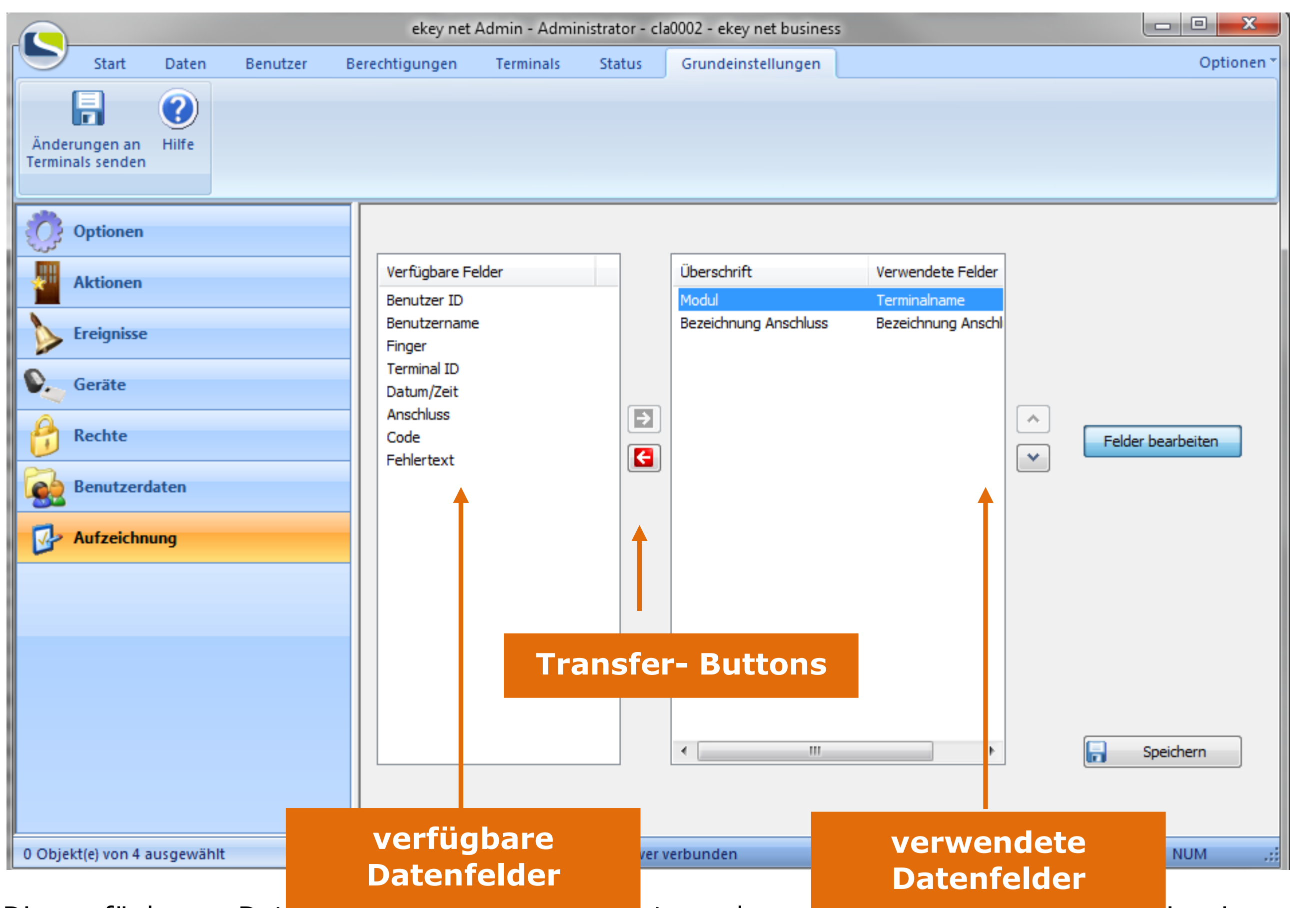
Hier definieren Sie, ob diese Systemmeldungen in das Logfile eingetragen werden.



15.1.2 Definition LOG-Inhalte für Masterserver CSV oder SQL

Neben dem internen ekey-Berichtswesen (SQL-Report im ekey-Programm) ist es auch möglich Ereignisse gesondert in eine andere SQL Datenbank zu schreiben und dort weiterzuverarbeiten (zb. Zeiterfassungsprogramme, Automatisierungen,…)
Hier ist zu definiieren bei welchen Ereignissen ein Logeintrag gemacht wird (siehe Kapitel 15.1.1.1) sowie auch die Datenfelder.
Sollte als „Art" nicht „Logdaten in ODBC speichern" gewählt worden sein, so beziehen sich die Inhalte der Spalten auf zb. die CSV Log-Datei des Masterservers.

Klicken Sie dazu auf den Command-Button [Felder bearbeiten], und es öffnet sich dieses Fenster.



Die verfügbaren Datenfelder sind die vom System ekey net möglichen Werte, die in einem Datensatz dann zusammengefasst werden.

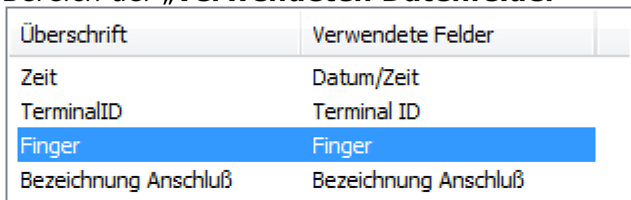
- Benutzer ID: „id" Die in den Eigenschaften des Benutzers und vom System definierte Benutzer ID
- Benutzername: „Name" der in den Eigenschaften des Benutzers definierte Name (Name +Vorname)
- Finger: „Finger" Nummer des verwendeten Fingers (1-10)
- TerminalID: „TerminalID" Interne ID des Fingerscanners bzw. der Steuereinheit
- Module: „Module" Terminalname
- Datum/Zeit: „Time" Datum und Uhrzeit im definierten Format
- Code: „ECode" Ereignis-Code wird intern vergeben
- Bezeichnung Anschluss: „Connection" Bezeichnung des Anschlusses



wein den Eigenschaften der Steuereinheit definiert

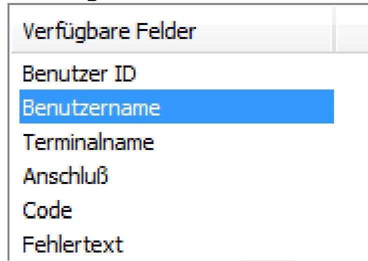
- Anschluss: „Relay“ Relaisnummer, die durch das Ereignis geschalten wird
- Fehlertext: „EText“ Nicht nur der Fehlertext wird hier eingetragen, sondern auch die Bezeichnung des Ereignisses.
- Personalnummer: „StaffID“Die in den Eigenschaften def. Personalnummer

Um nun ein Datenfeld einem Datensatz zuzuordnen, wählen Sie als erstes die Position im Bereich der „**verwendeten Datenfelder**“

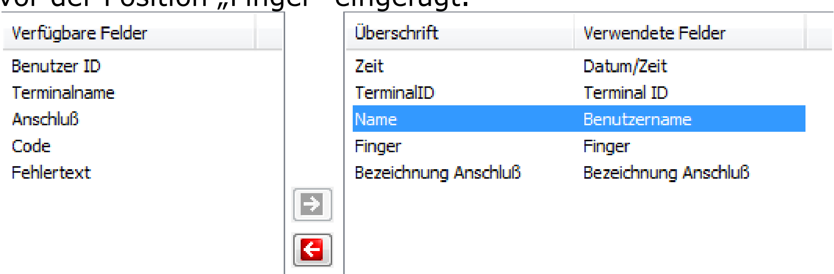


Hier z.B. wird ein neues Feld oberhalb der Position des „Finger“ eingefügt. „Finger“ und „Bezeichnung Anschluss“ rutschen dann um eine Zeile nach unten.

Wählen Sie hier das Datenfeld das Sie in ihren Datensatz mit aufzeichnen wollen, im Bereich „verfügbare Datenfelder“ mit einem linken Mausklick.



und klickenSie . Der Datenwert wandert dann in den Bereich der „verwendeten Datenfelder“ an die gewählte Position. In diesem Beispiel wird das Datenfeld „Benutzername“ vor der Position „Finger“ eingefügt.



Öffnen Siespäter das Logfile (.csv) dann z.B. mit MS Office Excel, so werden die Datenfelder wie folgt den Spalten zugewiesen.



	A	B	C	D	E	F
1	Zeit	TerminalID	Name	Finger	Bezeichnung Anschluß	

Ändern Sie die Reihenfolge der Datenfelder auf ein bereits bestehendes Logfile (.csv), so werden die bereitsbestehenden Einträge nicht mehrgeändert! Die Reihung der

Datenfelder verbleibt wie ursprünglich definiert. Die neuen Einträge werden entsprechend der Neudefinition gereiht. Ändern Sie also ihre Datensätze, legen Sie bitte auch immer ein neues Logfile an!

15.1.3 Aufzeichnung Masterserver

Logdaten werden hier von der gesamten ekey net Struktur gesammelt

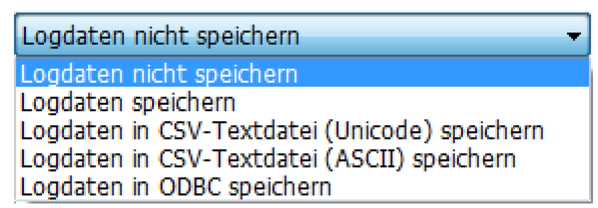
Logging Master Server	
Logging Data	Save log data in CSV text file (ASCII)
Path for csv log file	c:\ekeylog.csv
DSN for database access (ODBC)	
User	
Password	
Log for Time _Attendance	c:\timelog.csv

Bei Verwendung der Funktion „Log für Zeiterfassung" ist folgendes zu beachten:
Sollte dem Benutzer eine Personalnummer zugewiesen worden sein, wird anstatt des Namens die Personalnummer gespeichert.

Folgende Konfigurationen können Sie hier vornehmen.

Logdaten	Logdaten nicht speichern

Wählen Sie hier die Art des Logging



Logdaten nicht speichern: Es werden keine Logdaten gespeichert.
Logdaten speichern: Logdaten werden gespeichert, aber im ekey-internen Format. Die Daten können dann in den Datenfenstern abgerufen werden. Ein Pfad ist dann folgend nicht einzugeben.
Logdaten in CSV-Textdatei (Unicode) speichern:Die Logdaten werden in einem .csv-File im UNICODE-Format abgespeichert.
Logdaten in CSV-Textdatei (ASCII) speichern:Die Logdaten werden in einem .csv-File im Format ASCII abgespeichert.
Logdaten in ODBC speichern:Die Logdaten werden mittels ODBC in eine Datenbank gespeichert (siehe dazu ODBC Logging- Kapitel 15.1.5).

Pfad für Logdaten	c:\ekey_TOCAnet_DB\LOG\simone_CSV_ASCII_2.c

Haben Sie eine der 2 Arten des CSV-Loggings gewählt, so geben Sie hier den Pfad, samtFile-Name und Extension ein. Achten Sie darauf, dassSie am gewählten Speicherort die entsprechenden Schreib- und Leserechte vorliegen.



Können Sie hier keine Einstellungen machen, so haben Sie ein Kennwort definiert. Klicken Sie aufund geben Sie das Kennwort ein. Anschließend sind alle Einstellungen möglich. Werkseitig ist kein Kennwort definiert.

DSN für Datenbankzugriff (ODBC)	
Benutzer	
Kennwort	

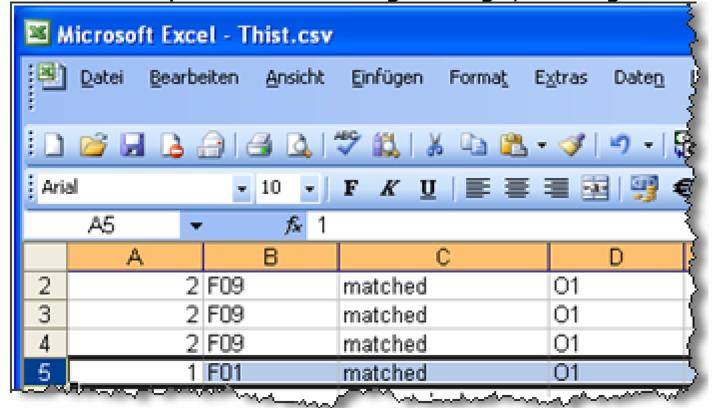
Diese Daten sind für das ODBC-Logging notwendig. Siehe dazu Kapitel 15.1.5



15.1.4 Nur positive Matchingeinträge im Log

Pfad zur Logdatei	D:\ekey net LOGs\ekey net Time Log.csv

Aus einer früheren ekey Anwendung haben wir diese Möglichkeit, Daten in einem spezifischen vordefinierten Format zu loggen, übernommen. Sie können, wenn Sie hier einen Pfad samt Filename und Extension eingeben, auch in diesem einfachen Format Daten aufzeichnen. Es werden nur positive Matchingeinträge, in foilgendem Format aufgezeichnet:



Im obigen Beispiel in Zeile 5 ist z.B. dokumentiert, dass der Benutzer mit ID 1 mit dem Finger F01 erkannt wurde und entsprechend Relais O1 geschaltet worden ist.
Das Format der Protokolldateien ist „csv" und kann sehr einfach z.B. mit Microsoft Excel geöffnet werden.

Sie müssen dann abschließend noch bei jedem ekey net FS definieren, ob Sie diesen in eben seine Daten mitloggen wollen. Aktivieren Sie dazu in den Eigenschaften des Fingerscanners die Checkbox:



15.1.5 ODBC/SQL Logging

15.1.5.1 SQL Datenbank

Mit ODBC (= **O**pen **Data**base **C**onnectivity)-Logging verschafft ihnen ekey net die Möglichkeit die Ereignisdaten aus ekey net direkt in eine SQL (=Structured Query Language) kompatible Datenbank zu schreiben und zu speichern.

Damit ist auch klar, dass Sie für ODBC–Logging eben eine SQL-kompatible Datenbank benötigen. Wir empfehlen Ihnen dafür z.B. Microsoft SQL Server 2005.

Bevor Sie die Einstellungen im ekey net machen, müssen Sie die SQL-Datenbank konfigurieren. Wir zeigen das hier am Beispiel Microsoft SQL 2005 Server.

Installieren Sie auf ihrem Zielsystem

- Microsoft SQL Server 2005
- Microsoft SQL Server Management Studio Express.

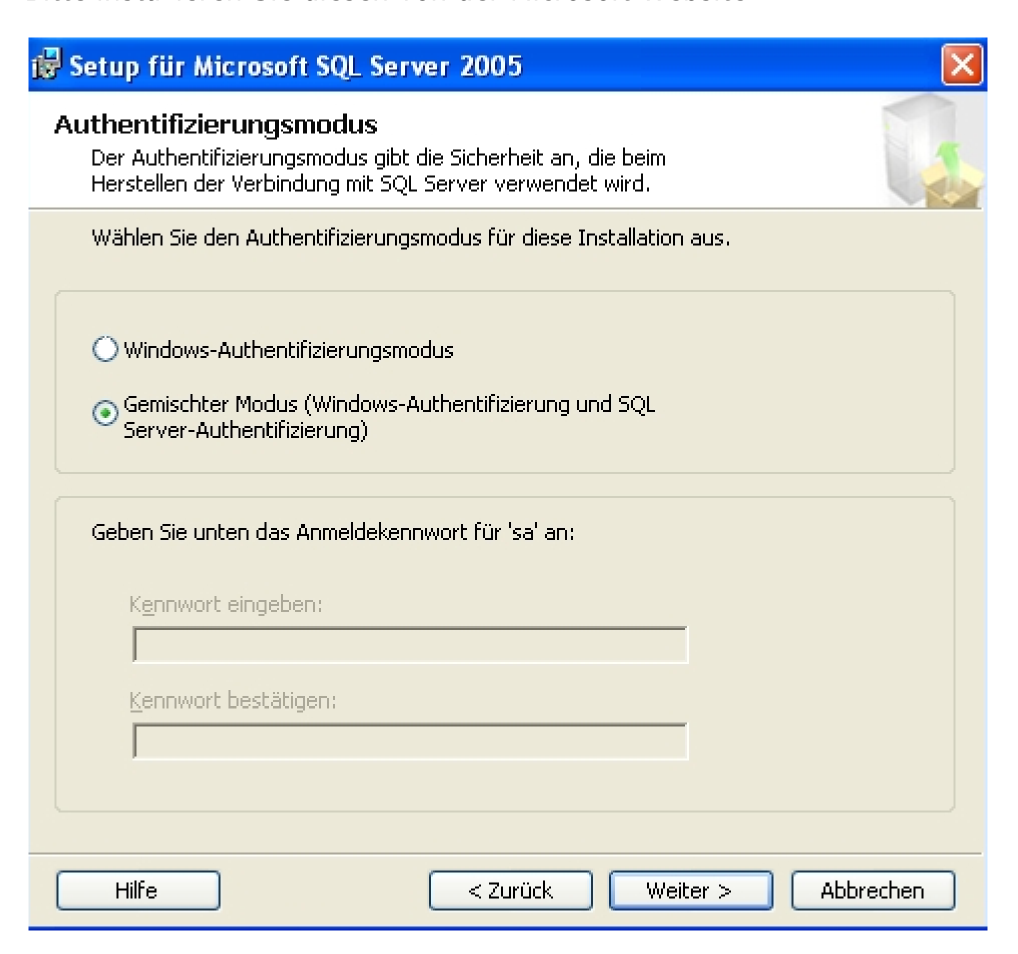
Wichtig ist, dass Sie beim Authentifizierungsmodus während der Installation von SQL Server 2005 „Gemischter Modus"(Windows Authentifizierung und SQL Server Authentifizierung) wählen, und einen **Benutzername und ein Passwort** definieren.



15.1.5.2 SQL Server& Management Studio Express

Microsoft bietet einen kostenlosen SQL Server an.

Bitte installieren Sie diesen von der Microsoft Website



Bei der Authentifizierungsmethode wählen Sie bitte „Gemischte rModus"

Der User ist bei dieser Software immer „sa". Vergebne Sie noch ein passwort.

Danach installieren sie bitte das Management Studio.

Microsoft SQL Server Management Studio Express (SSMSE) ist ein kostenloses, leicht zu verwendendes grafisches Verwaltungstool zum Verwalten von SQL Server 2005 Express Edition und SQL Server 2005 Express Edition with Advanced Services. Das Tool ist bei www.microsoft.com downloadbar. Für die Beschreibung der ekey net ODBC-Logging Funktionen verwenden wir beispielhaft dieses Tool.

Installieren Sie das Tool auf ihrem Zielrechner.

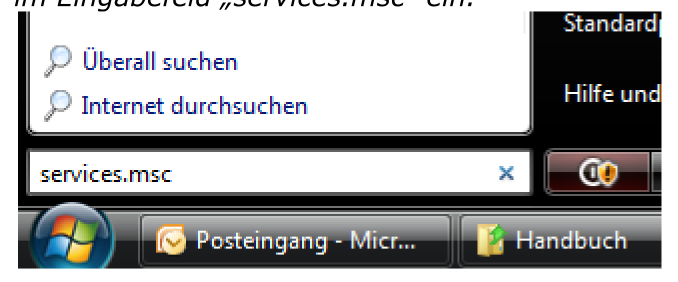


Achten Sie dabei, dass der installierende Benutzer volle Schreibrechte am Installationsverzeichnis hat. Ein Benutzer mit Adminrechten genügt NICHT!

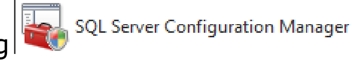
Prüfen Sie nun, ober der Windows-Dienst SQL Server Browser aktiviert und gestartet ist. Ist das nicht der Fall aktivieren und starten Sie ihn.



Um zur Verwaltung der Windowsdienste zu gelangen klickenSie auf Start und geben Sie im Eingabefeld „services.msc" ein.



15.1.5.3 Datenbankverbindung

Starten Sie nun aus dem Programmverzeichnis die Anwendung 

Die Dienste

- SQL Server-Browser
- SQL Server(SQLEXPRESS)

müssen aktiviert sein und laufen. Sie sehen das im rechten Fenster des untenstehenden Screenshots
Status: „wird ausgeführt"

SQL Server Configuration Manager
Datei Aktion Ansicht ?
Maximiere
SQL Server-Konfigurations-Manager (Lokal)
SQL Server 2005-Dienste
SQL Server 2005-Netzwerkkonfiguration
SQL Native Client-Konfiguration

Name	Status	Startmodus	Anmelde
SQL Server-Browser	Wird ausgeführt	Automatisch	NT AUTH
SQL Server (SQLEXPRESS)	Wird ausgeführt	Automatisch	NT AUTH

Starten Sie **SQL Server Oberflächenkonfiguration** aus dem Programmverzeichnis
SQL Server-Oberflächenkonfiguratic
.



SQL Server 2005-Oberflächenkonfiguration

Microsoft SQL Server 2005

Windows Server System

Schützen von SQL Server

Minimieren der SQL Server 2005-Oberfläche

SQL Server 2005 verbessert die Verwaltbarkeit und Sicherheit, indem Administratoren mehr Kontrolle über die Oberfläche von lokalen Instanzen und Remoteinstanzen von SQL Server 2005 erhalten. Die SQL Server 2005-Oberflächen-Konfigurationstools ermöglichen Folgendes:

- Deaktivieren nicht verwendeter Dienste und Netzwerkprotokolle für Remoteverbindungen.
- Deaktivieren nicht verwendeter Features von SQL Server-Komponenten.

Für Neuinstallationen aktivieren Sie mithilfe dieser Tools erforderliche Features, Dienste und Netzwerkprotokolle, die standardmäßig deaktiviert sind. Für aktualisierte Instanzen identifizieren und deaktivieren Sie mithilfe dieser Tools nicht verwendete Features, Dienste und Protokolle.

Add New Administrator

Weitere Informationen zum Konfigurieren der SQL Server-Oberfläche.

Oberfläche konfigurieren für localhost (Computer wechseln)

Oberflächenkonfiguration für Dienste und Verbindungen

Oberflächenkonfiguration für Features

Klicken Sie nun auf Oberflächenkonfiguration für Dienste und Verbindungen und stellen Sie bei den Remoteverbindungen auf **TCP/IP und Named Pipes.**

Starten Sie anschließend im **SQL Server Configuration Manager** den Dienst **SQL Server Browser** neu.

Oberflächenkonfiguration für Dienste und Verbindungen - localhost

SQL Server 2005 Surface Area Configuration
Schützen von SQL Server

Aktivieren Sie nur die von Ihren Anwendungen verwendeten Dienste und Verbindungstypen. Durch das Deaktivieren nicht verwendeter Dienste und Verbindungen wird die Oberfläche reduziert und dadurch Ihr Server geschützt. Die Standardeinstellungen finden Sie unter Hilfe.

Wählen Sie eine Komponente aus, und konfigurieren Sie ihre Dienste und Verbindungen:

NET2
Database Engine
Dienst
Remoteverbindungen
OFFICESERVERS
SQL Server Browser
Dienst

Standardmäßig ermöglichen SQL Server 2005 Express Edition, SQL Server 2005 Evaluation Edition und SQL Server 2005 Developer Edition nur lokale Clientverbindungen. SQL Server 2005 Enterprise Edition, SQL Server 2005 Standard Edition und SQL Server 2005 Workgroup Edition überwachen außerdem Remoteclientverbindungen über TCP/IP. Mit den Optionen unten können Sie die Protokolle ändern, die von SQL Server auf eingehende Clientverbindungen überwacht werden. TCP/IP ist Named Pipes vorzuziehen, weil für dieses Protokoll weniger Ports über die Firewall geöffnet werden müssen.

Nur lokale Verbindungen
Lokale Verbindungen und Remoteverbindungen
Nur TCP/IP verwenden
Nur Named Pipes verwenden
TCP/IP und Named Pipes verwenden

Nach Instanz anzeigen | Nach Ko

OK | Abbrechen | Anwenden | Hilfe

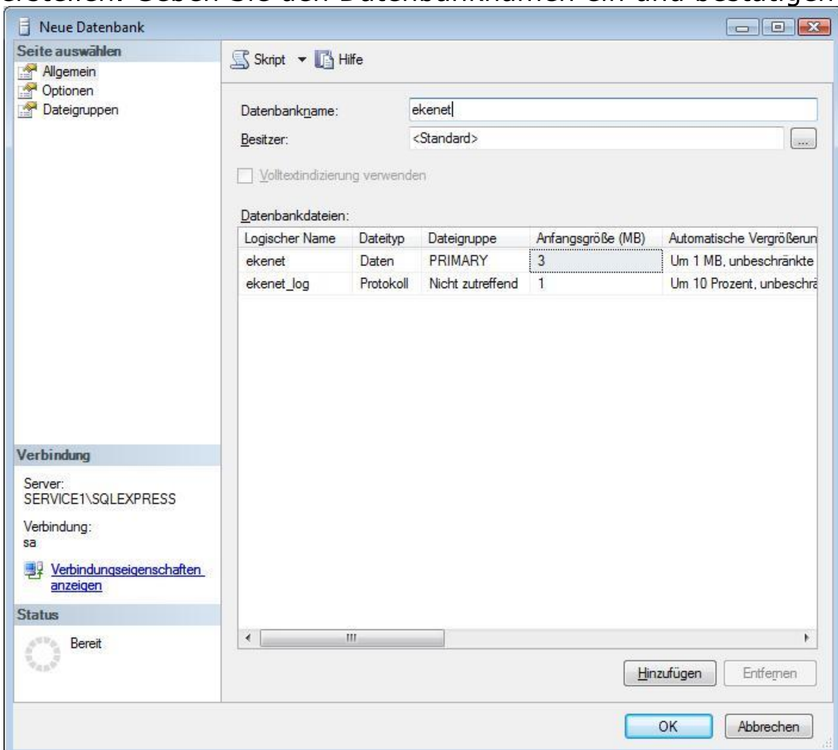
Starten Sie nun **SQL Server Management Studio Express**. Stellen Sie dort auf Authentifizierung auf SQL Server-Authentifizierung und geben Sie Anmeldename und Passwort wie unter Kapitel 15.1.5.1 definiert ein.





15.1.5.4 Datenbank erstellen

Machen Sie nun einen Rechtsklick auf „**Datenbank**" und wählen Sie eine „**neue Datenbank"** erstellen. Geben Sie den Datenbanknamen ein und bestätigen Sie mit OK.



15.1.5.5 Tabellen erstellen

Wählen Sie nun mit einem Rechtsklick die neue Datenbank und erstellen Sie eine **Abfrage** mit folgendem Code. Schließen Sie die Eingabe mit „)"ab.

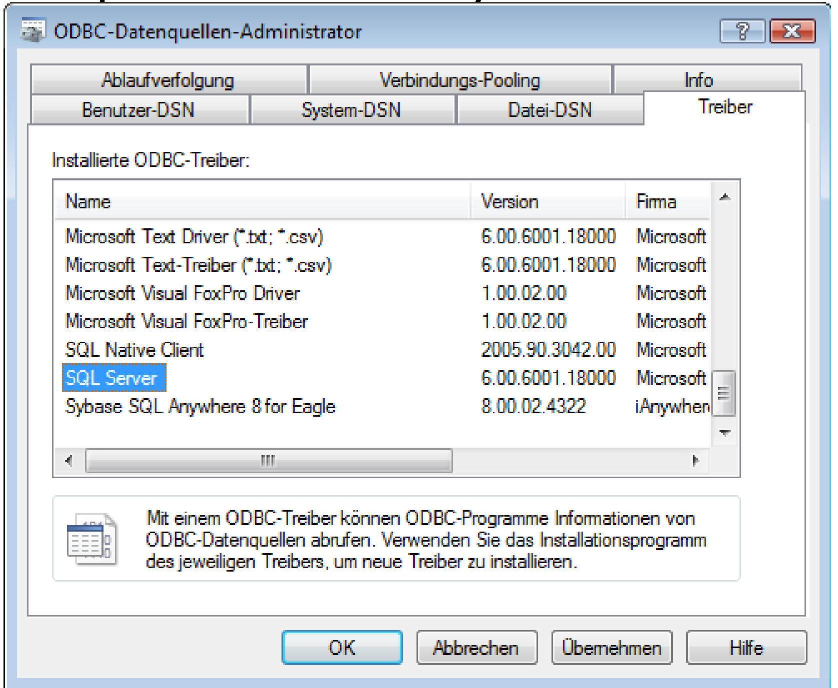
```
CREATE TABLE EkeyNetLog
(
        UserID int,
        UserName varchar (255),
        FingerID int,
        TerminalID int,
        TerminalName varchar (255),
        EvtTime varchar (50),
        RelayID int,
        RelayName varchar (255),
        EvtCode int,
        EvtText varchar (255)
)
```

Falls sie bei den Benutzerprofilen weitere Informationen wie Personalnummer oder E-Mail gewählt haben, stehen diese bei den Optionen auch zur auswahl und sind hier ggf. einzubauen.

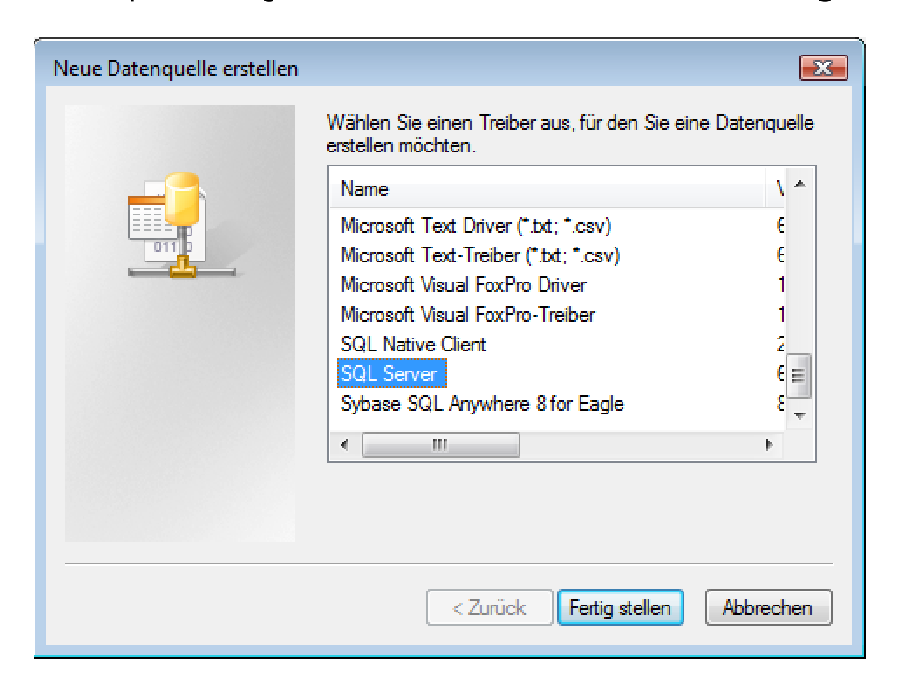


15.1.5.6 ODBC Verbindung zur SQL Datenbank erstellen

Öffnen Sie die Windows – **Systemsteuerung**und wählen Sie **Verwaltung** Verwaltung – **Datenquellen ODBC.** Im Reiter„**System - DSN**" wählen Sie „**hinzufügen**".

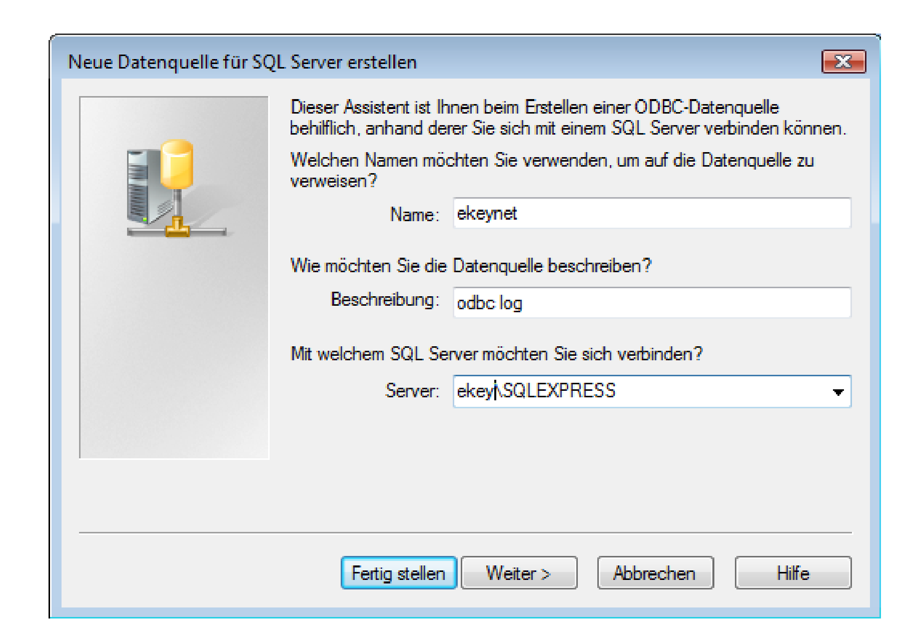


Datenquelle „**SQL Server**" auswählen und mit „**Fertig stellen**" abschließen.

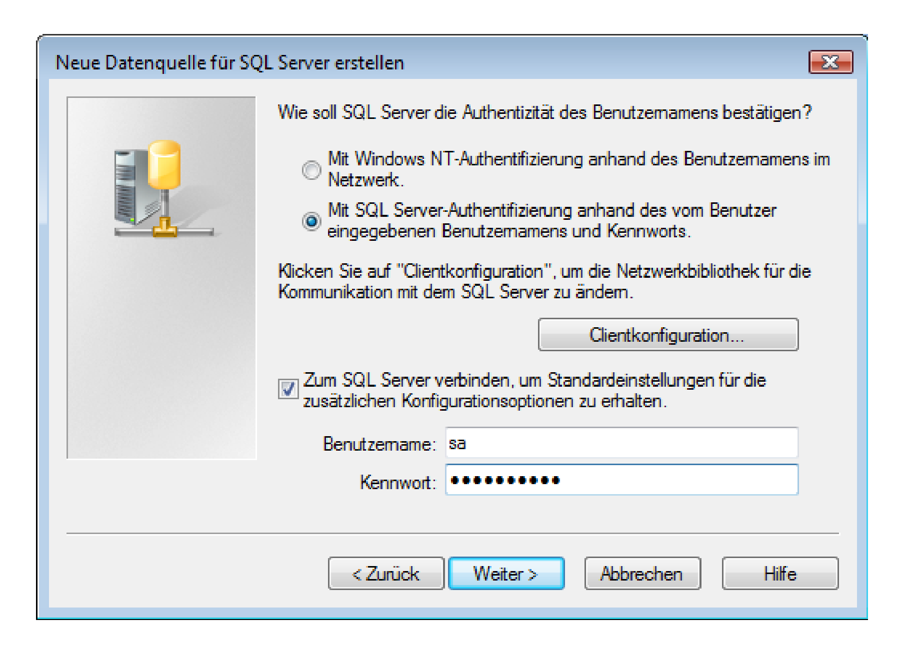


Geben Sie nun den Datenbanknamen ein (= **Name der dann auch im ekey net Admin einzugeben ist!)** und unter Server den „**Hostnamen"\SQLEXPRESS.** Schließen Sie mit „**Weiter**>" die Eingabe ab.

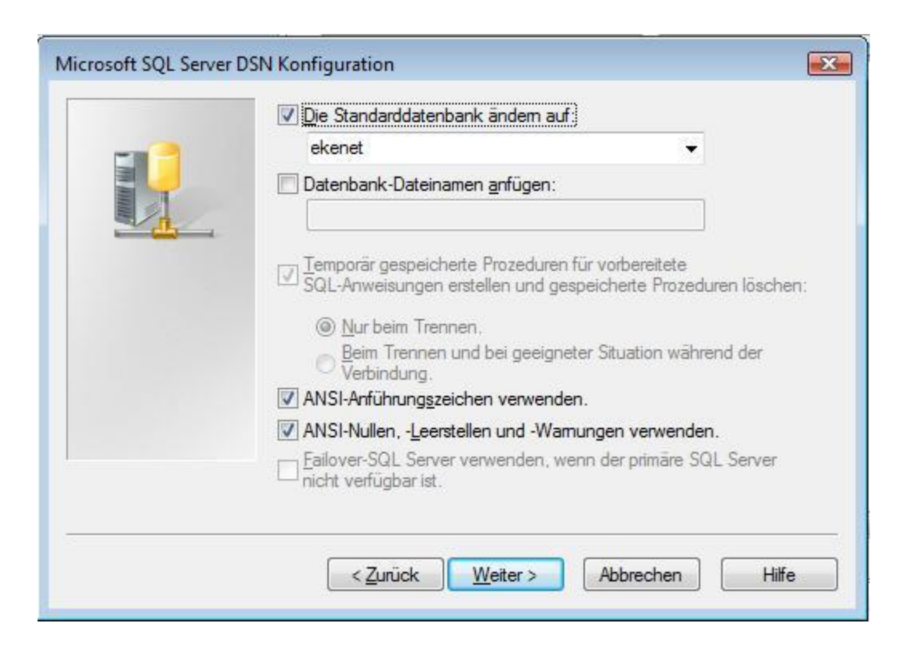




Wählen Sie nun „**Mit SQL Server-Authentifizierung anhand…..**" und geben Sie Benutzername und Passwort wieder ein, wie unter 15.1.5.1 bereits definiert. Schließen Sie die Eingabe wieder ab mit Klick auf„**Weiter >**".



Abschließend stellen Sie die Standarddatenbank auf die neu angelegte Datenbank („ekeynet") um und schließen Sie mit „Weiter" ab.

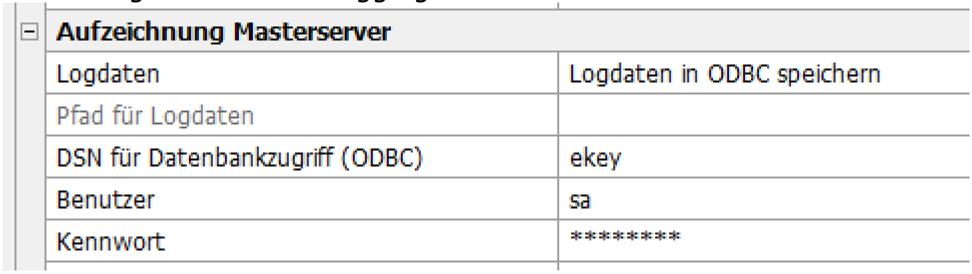


15.1.5.7 Einstellungen im ekey net Admin



Definieren Sie als erstes die Datensätze lt. Kapitel 15.1.2. Ohne diese Definition werden keine Daten zur Datenbank gesandt.

Im ekey net Admin unter „**Aufzeichnung**" und Bereich Aufzeichnung Masterserver sind die Einstellungen für ODBC-Logging zu machen.



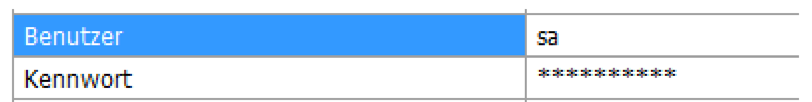
Aufzeichnung Masterserver	
Logdaten	Logdaten in ODBC speichern
Pfad für Logdaten	
DSN für Datenbankzugriff (ODBC)	ekey
Benutzer	sa
Kennwort	********

Logdaten	Logdaten in ODBC speichern

Wählen Sie bei Logdaten „Logdaten in ODBC speichern"

DSN für Datenbankzugriff (ODBC)	ekey

Geben Sie hier den Datenbanknamen ein, wie unter 15.1.5.4beschrieben.



Benutzer	sa
Kennwort	**********

Hier geben Sie noch Benutzername und Kennwort wie unter 15.1.5.1 definiert ein

Nach allen Eingaben schließen Sie mitab.

Damit sind alle Einstellungen für ODBC-Logging gemacht und die Logdaten werden direkt in die SQL kompatible Datenbank abgelegt.

15.1.6 Aufzeichnung Statusfenster

Hier geben Sie die Grundeistellungen für die Anzeige der Daten im Status definieren:

Maximale Zeilen Logdatei	50000

Die maximale Anzahl der im Log gespeicherten Zeilen – wird dieser Wert überschritten, so wird automatisch 1/8 der ältesten Einträge gelöscht.

Maximum übertragene Zeilen	1000

Die maximale Anzahl der übertragenen Zeilen bei Ausführen einer Suchaktion im Statusfenster. Je höher dieser Wert ist, desto mehr Daten müssen beim Start des ekey net Admin in den Arbeitsspeicher geladen werden und beeinflussen damit die Geschindigkeit bei der Anmeldung an der ekey net Datenbank.

Maximum angezeigte Zeilen	1000

Die maximale Anzahl der sichtbaren Zeilen im Statusfenster. Je höher dieser Wert ist, desto mehr Daten müssen im Arbeitsspeicher verwaltet werden und beeinflussen damit die Geschindigkeit während der Arbeit in der ekey net Datenbank.

15.1.7 Web-Aufzeichnung

Logdaten können aus ekey net auch über das www an eine definierte Adresse versandt werden. Um Weblogging zu aktivieren gehen Sie wie folgt vor:

Wenn ein Kennwort für die Aufzeichnungskontrolle aktiviert wurde geben Sie unter**Grundeinstellungen** ->**Aufzeichnung** das Passwort für die Aufzeichnungskontrolle ein

Aufzeichnung	
Kennwort Aufzeichnungskontrolle	****

Anschließend aktivieren Sie die Webaufzeichnung durch klick auf die Checkbox **Webaufzeichnung**

Web-Aufzeichnung	
Web-Aufzeichnung	☑ Ja

Sie können nun die Feldbezeichnungen der Aktionscodes anpassen:

Web Logging	
Web Logging	☑ Yes
Use only action code containing text	☐ No
Action Code 'Access'	Zutritt
Action Code 'Departing'	Verlassen
Action Code 'Denied'	Ablehnung
Action Code 'Unknown finger'	Unbekannter Finger
Action Code 'Alarm On'	Alarm ein
Action Code 'Alarm Off'	Alarm aus



Um nun die Zieladresse und dieInhalte der LOG-Daten zu definieren klicken Sie auf den Button

Web-Aufzeichnung

Folgendes Fenster öffnet sich:

ekey net Admin - Administrator - cla0002 - ekey net business

Start | Daten | Benutzer | Berechtigungen | Terminals | Status | Grundeinstellungen | Optionen

Änderungen an Terminals senden | Hilfe

Optionen
Aktionen
Ereignisse
Geräte
Rechte
Benutzerdaten
Aufzeichnung

http://adresse.com/x.htm?par=

Adressfeld

Verfügbare Felder
id
Name
Finger
TerminalID
Modul
Zeit
Relais
Bezeichnung Anschluss
ECode
EText
Personalnummer
E-Mail
Telefon
Mobiltelefon
Adresse
Titel

Geben Sie hier die Web-Adresse mit allen notwendigen Parametern ein.
Fügen Sie Felder mit einem Doppelklick aus der Liste ein.

Web-Aufzeichnung

Parameter

Speichern

0 Objekt(e) von 4 ausgewählt | ekey net business Lizenzen - ge | Server verbunden | Neu verbinden | NUM

Geben Sie im Adressfeld die Zieladresse der Logdaten ein und schließen Sie die Adresse mit einem „**/**" ab.z.B. **http://www.ekey.net/**.

Nun definieren Sie die Logdatensätze, die Sie an die oben genannte Adresse senden möchten. Machen Sie einfach einen Doppelklick auf den gewünschten Parameter in der Liste und trennen Sie jeden Parameter mit dem Trennzeichen „**&**".

Folgende Parameter können Sie übernehmen:

id	Telefon	
Name	Mobiltelefon	
Finger	Adresse	Monat mit führender 0
TerminalID	Titel	Monat
Modul	Position	Tag mit führender 0
Zeit	Abteilung	Tag
Relais	Vorgesetzter	Stunde mit führender 0
Bezeichnung Anschluß	Assistent	Stunde
ECode	Aktionscode	Minute mit führender 0
EText	Konto	Minute
Personalnummer	Jahr 4-stellig	Sekunde mit führender 0
E-Mail	Jahr 2-stellig	Sekunde



Hier ein Beispiel:

http://10.1.28.28/pwclient/OpenPrinterFromEkey.asp?username=**»UserName»**&personalnummer=**«StaffID»**

An die Adresse 10.1.28.28/pwclient
Wird bei einem Ereignis:

- Der Benutzername
- Die Personalnummer

gesendet.

Auf Empfängerseite, können diese Meldungen dann verarbeitet werden. Sie brauchen dazu natürlich eine entsprechende Anwendung die diese Logdaten verarbeiten kann.

Aktivieren Sie noch bei den gewünschten ekey net FS die Funktion Web-Aufzeichnung:

Web-Aufzeichnung	☐

Siehe Kapitel 6.6.3.2.3.2



Nach einem Update von ekey net 3.x auf ekey net 4.x müssen Sie die Web-Aufzeichnung an den genwünschten ekey net FS aktivieren In den Vorgängerversionen wurde automatisch von allen ekey net FS aufgezeichnet.

15.1.8 Berichtswesen (auf SQL Basis)

Um das ekey Software Interne Berichtswesen, wie unter „Punkt 6.3.2 Berichte über Benutzer- oder Fingerscanneraktivitäten") nutzen zu können, gehen Sie bitte wie folgt vor:

1. Installation eines SQL-Server
   Eine kostenlose Version von „*Microsoft SQL Server* 2005 Express Edition" kann auf der Internetseite von Microsoft heruntergeladen werden.

2. Installation von „*Microsoft SQL* Server *Management* Studio Express"
   kann auf der Internetseite von Microsoft heruntergeladen werden.
   siehe Punkt 15.1.5.2

3. ODBC-Schnittstelle konfigurieren
   siehe Punkt 15.1.5.6 ODBC Verbindung zur SQL Datenbank erstellen

Die Inhalte dieser SQL Datenbank können dann auch von externen Systemen ausglesen werden, wie z.B.: Crystal Reports.

Aktivieren Sie nun die Checkbox und füllen Sie die Zugangsdaten aus:

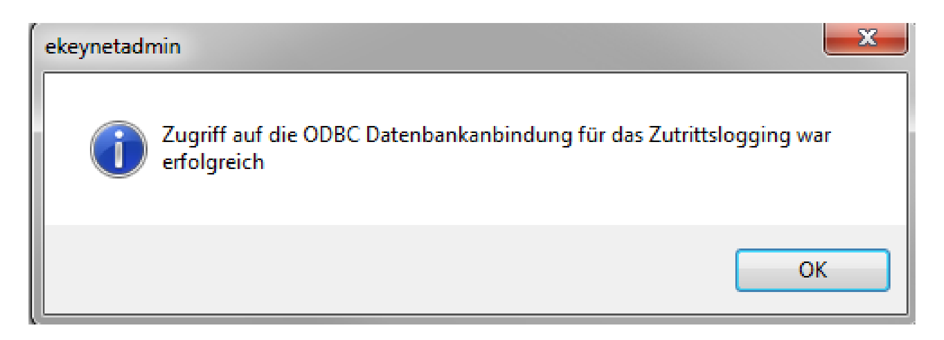
Berichtswesen	
Berichtswesen aktivieren	☑
DSN	ekey
Benutzername	Administrator
Kennwort	**********

© 2010 – ekey biometric systems GmbH



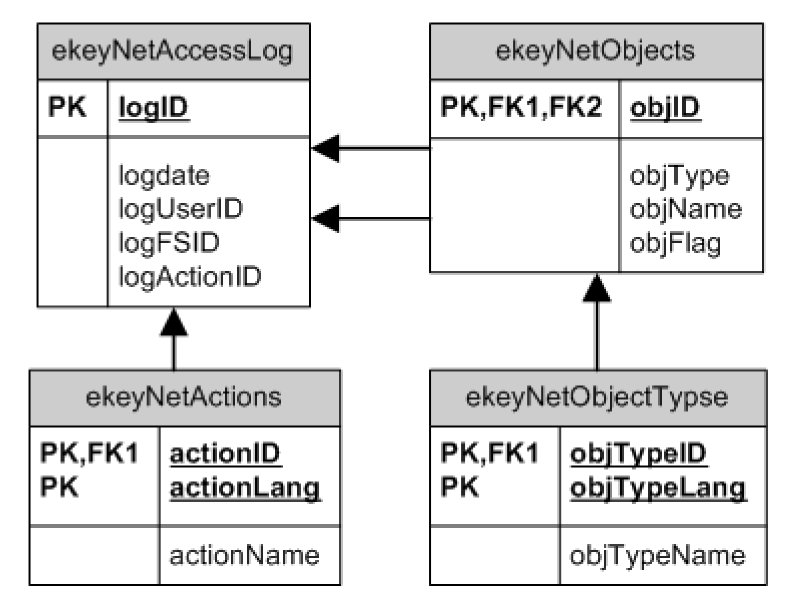
Reporting
Test/Configure ...

Durch Klick auf die Schaltfläche werden die nötigen Tabellen in der Datenbank automatisch angelegt und mit dieser Systemmeldung bestätigt:



Folgende Tabellenstruktur wird vom System angelegt und wird nun von der Funktion zur Erstellung von Berichten – Kapitel 6.3.2 verwendet – steht aber auch jeder externen Berichtssoftware zur Verfügung. Die Funktionalität setzt eine MS SQL kompatible Datenbank voraus und wurde auf My SQL, MS SQL und MS Access getestet.

Dieses ER-Diagramm liegt dem Aufbau der Datenbank zugrunde:



Daraus ergeben sich folgende Tabellen:

- Tabellen
  - Systemtabellen
  - dbo.ekeyNetAccessLog
  - dbo.ekeyNetActions
  - dbo.ekeyNetObjects
  - dbo.ekeyNetObjTypes

ekeyNetAccessLog

logId	logDate	logUserId	logFsId	logActionId
1	24.03.2010 09:20:33	101	1049687	1
2	24.03.2010 09:21:00	103	1049616	1

ekeyNetActions

actionId	actionLang	actionName
1	DEU	Impuls Anschluss 1
2	DEU	Impuls Anschluss 2
3	DEU	Impuls Anschluss 3
4	DEU	Impuls Anschluss 4
5	DEU	Anschluss 1 ein
6	DEU	Anschluss 2 ein
7	DEU	Anschluss 3 ein
8	DEU	Anschluss 4 ein
9	DEU	Anschluss 1 aus

ekeyNetObjects

objId	objType	objName	objFlag
1	30	Administrator	0
101	30	Pichler, Günther	0
102	30	Mustermann, Max	0
103	30	Huber, Hans	0
1049578	32	Immer	0
1049579	33	Kalender Deutschland	1
1049580	33	Kalender Großbritannien	1
1049581	33	Kalender Irland	1
1049582	33	Kalender Italien	1
1049583	33	Kalender Kanada	1

objFlag 0 = aktives Objekt
objFlag 1 = gelöschtes Objekt

ekeyNetObjTypes

objTypeId	objTypeLang	objTypeName
1	DEU	ekey net S Fingerscanner
2	DEU	ekey net M Fingerscanner
3	DEU	ekey net L Fingerscanner
4	DEU	ekey net S integra Fingerscanner
5	DEU	ekey net M integra Fingerscanner
6	DEU	ekey net L integra Fingerscanner
7	DEU	ekey net S RFID-Fingerscanner
8	DEU	ekey net M RFID-Fingerscanner



16 Bereichsgrenzen

16.1 Allgemein

Im ekey net ist es auch möglich, Ereignisse und darauf folgende Aktionen zu definieren, die Schaltungen innerhalb eines Bereiches für alle Geräte gemeinsam ausführen. So können Sie zum Beispiel mit einem Fingerscan automatisch alle Türen im Bereich öffnen.
Bereiche im ekey net sind durch die Bereichsgrenzen definiert. Bereichsgrenzen können sein:

- ekey CVLAN
- ekey net Terminalserver
- ekey net Terminalgruppe

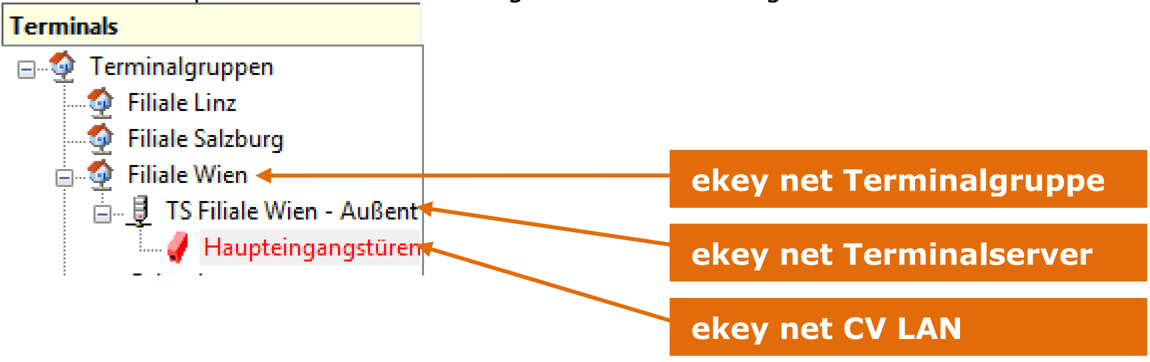
Wird z.B. ein ekey CVLAN als Bereichsgrenze definiert,so gehören alle Geräte (Fingerscanner und SE) die unter ihm angeordnet sind, zum Bereich. Eine Bereichs-Aktion (bzw. ein Ereignis) welches dann innerhalb dieser Gerätegruppe ausgelöst wird, wirkt dann auf alle Geräte in diesem Bereich.



ACHTUNG! Die „Bereichs-Aktion" sucht in der Struktur nach Oben bis zur nächsten Bereichsgrenze – Sollte KEINE Bereichsgrenze gesetzt ein, so würde theoretisch das gesamte ekey net System betroffen sein und alle ekey net SE schalten. Um dies zu verhindern wird bei KEINER konfigurierten Bereichsgrenze **automatisch der übergeordnete ekey net CV LAN** als Bereichsgrenze festgelegt.

16.2 Definieren der Bereichsgrenzen

Im Terminalexplorer sind die Bereichsgrenzen und die Organisation ersichtlich.



In den Eigenschaften dieser Terminalpositionen findet man die Möglichkeit diese als Bereichsgrenze zu aktivieren.

Bereichsgrenze Aktionen	☑



16.3 Definition der Aktion für Bereichsgrenze

Legen Sie unter „Grundeinstellungen" -> „Aktion" eine neue Aktion durch Klick auf
+ Klicken Sie hier für einen neuen… an, und definieren Sie anschließend die Eigenschaften.

Die grundsätzlichen Eingaben und Definitionen lesen Sie bitte im Kapitel 8.1.2 Für die Bereichsfunktionen maßgeblich ist ausschließlich die Einstellung bei der Eigenschaft.

Gerät	Alle Geräte im Bereich - Anschluss 1

Hier definieren Sie nun, welcher Aktor (= Relais) an jeder ekey net SE im Bereich schalten soll.

Alle Geräte im Bereich - Anschluss 1

Kein Gerät
Zugeordnetes Gerät - Anschluss 1
Lokales Gerät - Anschluss 1
Alle Geräte im Bereich - Anschluss 1
Zugeordnetes Gerät - Anschluss 2
Lokales Gerät - Anschluss 2
Alle Geräte im Bereich - Anschluss 2
Zugeordnetes Gerät - Anschluss 3
Lokales Gerät - Anschluss 3
Alle Geräte im Bereich - Anschluss 3
Zugeordnetes Gerät - Anschluss 4
Lokales Gerät - Anschluss 4
Alle Geräte im Bereich - Anschluss 4

Wollen Sie Bereichsaktionen definieren müssen Sie das Gerät entsprechend parametrieren und

- alle Geräte im Bereich – Anschluss 1 (wirkt auf Relais 1 der Steuereinheit) oder
- alle Geräte im Bereich – Anschluss 2 (wirkt auf Relais 2 der Steuereinheit) oder
- alle Geräte im Bereich – Anschluss 3 (wirkt auf Relais 3 der Steuereinheit) oder
- alle Geräte im Bereich – Anschluss 4(wirkt auf Relais 4 der Steuereinheit)

wählen.



Die Anzahl der verfügbaren, schaltbaren Anschlüsse (Relais) hängt vom verwendeten Gerätetyp ab.

16.4 Ereignisdefinition und Bereiche

Die grundsätzlichen Eingaben und Definitionen lesen Sie bitte im Kapitel 8.1.2.

Externes Ereignis bearbeiten	
Beschreibung	Fertigung - Alle Türen Schalten
Aktion	Bereich Impuls A1
Zähler	0

Definieren Sie ein neues Ereignis und weisen Sie diesem die Bereichsaktion zu. Hier im Beispiel wollen wir alle Türen der Fertigung dauerhaft öffnen.

Bei den Ereignissen darf immer nur im Feld

Aktion	Bereich Impuls A1

eine Aktion definiert werden, die in Bereichen wirkt.

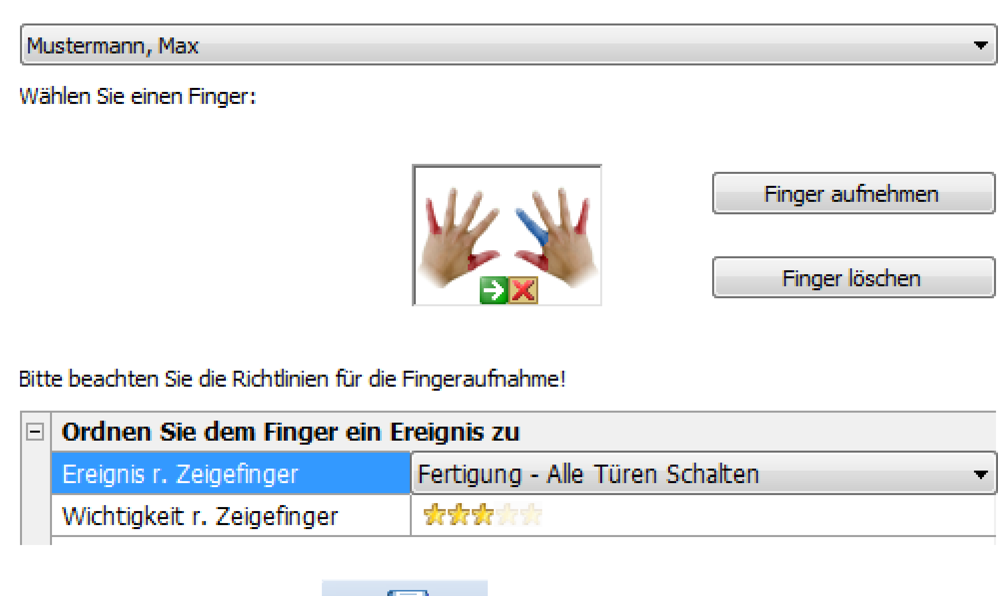
Definieren Sie bei
Aktion bei Zählerende
eine „**Bereichs**"-Aktion, so wird diese Aktion nur auf dem Fingerscanner ausgeführt, auf dem der Finger gezogen wird. Bei den Geräten im Bereich bleibt dies wirkungslos.



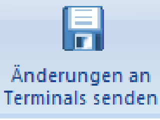
2 Aktionen gleichzeitig können also im „Bereich" nicht ausgeführt werden!!!

16.5 Zuweisung an Finger und Benutzer

Zuletzt weisen Sie das „**Bereichs**"-Ereignis dem Finger des entsprechenden Benutzers zu



Und klicken Sie auf



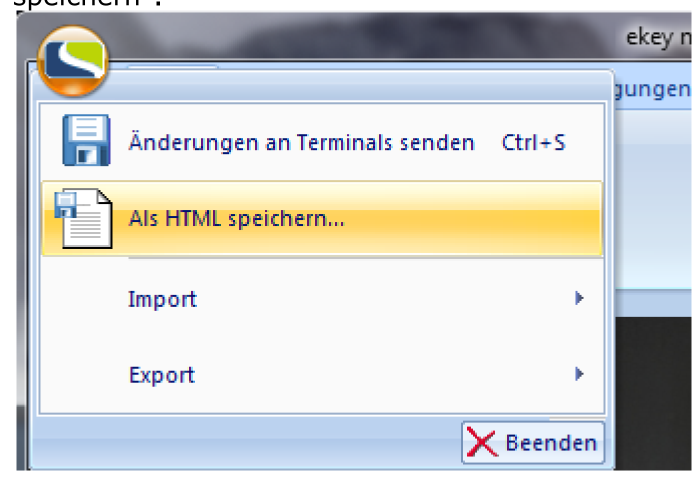


17 Alarmpläne

ekey net Alarmpläne sind seit Version 4.2 nicht mehr verfügbar.

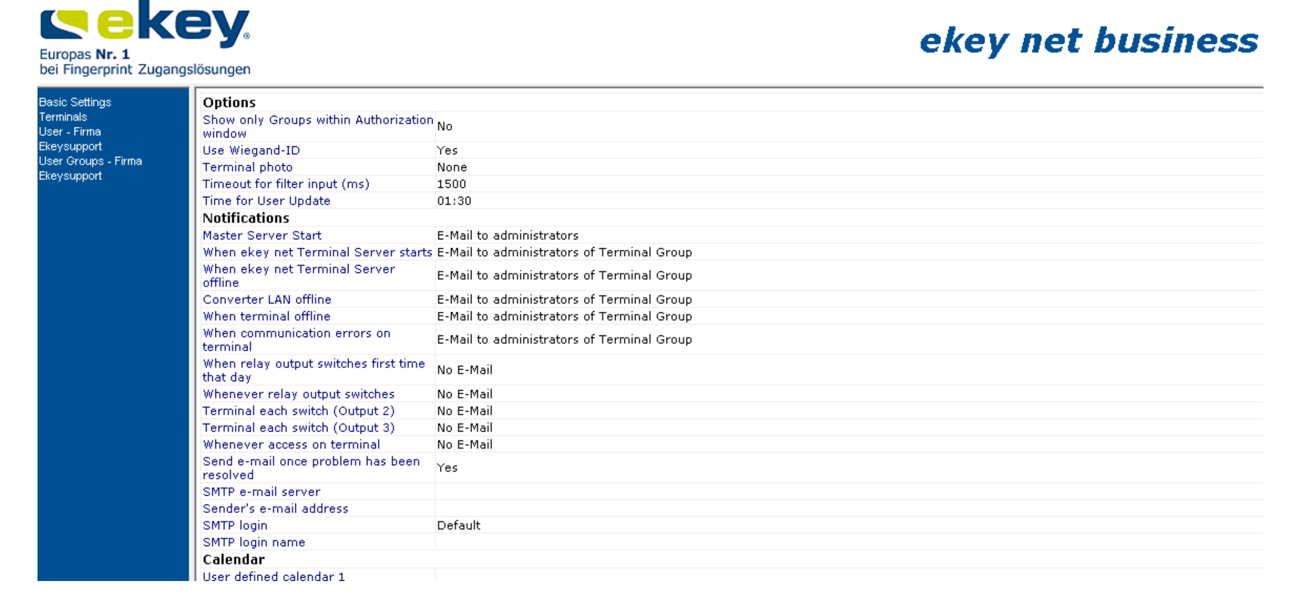
18 Als HTML speichern

Für Dokumentationszwecke können die Einstellungen und Parametrierungen des gesamten Systems im HTML Format exportiert werden. In der Dokumentation sind aber keine Fingerdaten enthalten.
Klicken Sie dazu mit der linken Maustaste auf das ekey Symbol und wählen Sie „als HTML speichern".



Der Speicherdialog von Windows öffnet sich, und Sie können wie gewohnt das HTML-File am gewünschten Speicherort mit gewünschtem Speichernamen ablegen.

Die Daten können Sie dann mit einem Standard Internet Browser (z.B. Internet Explorer) einsehen.
Hier ein Beispiel:


ekey
Europas Nr. 1
bei Fingerprint Zugangslösungen

ekey net business

Basic Settings
Terminals
User - Firma
Ekeysupport
User Groups - Firma
Ekeysupport

Options	
Show only Groups within Authorization window	No
Use Wiegand-ID	Yes
Terminal photo	None
Timeout for filter input (ms)	1500
Time for User Update	01:30
Notifications	
Master Server Start	E-Mail to administrators
When ekey net Terminal Server starts	E-Mail to administrators of Terminal Group
When ekey net Terminal Server offline	E-Mail to administrators of Terminal Group
Converter LAN offline	E-Mail to administrators of Terminal Group
When terminal offline	E-Mail to administrators of Terminal Group
When communication errors on terminal	E-Mail to administrators of Terminal Group
When relay output switches first time that day	No E-Mail
Whenever relay output switches	No E-Mail
Terminal each switch (Output 2)	No E-Mail
Terminal each switch (Output 3)	No E-Mail
Whenever access on terminal	No E-Mail
Send e-mail once problem has been resolved	Yes
SMTP e-mail server	
Sender's e-mail address	
SMTP login	Default
SMTP login name	
Calendar	
User defined calendar 1	



19 UDP-Versand

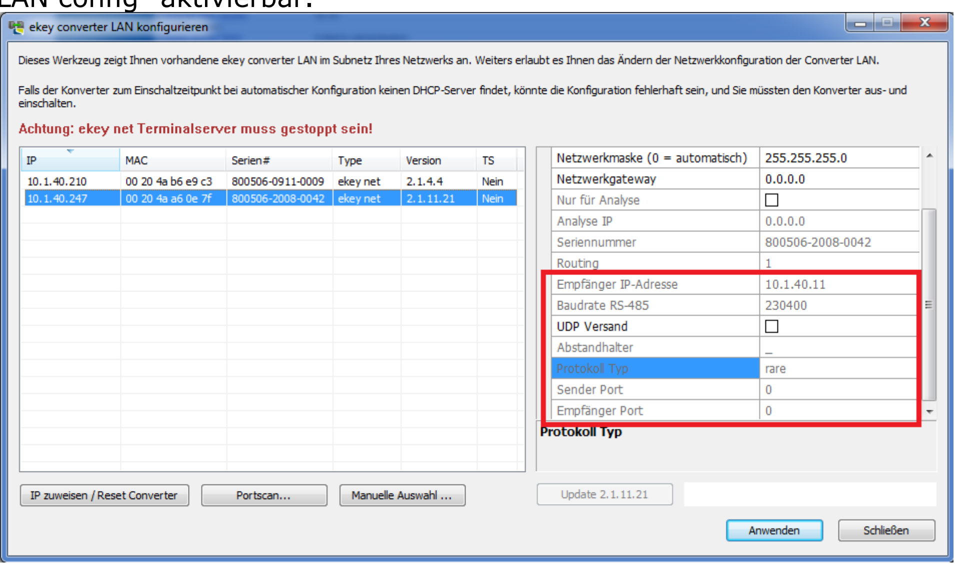
19.1 UDP-Versand durch ekey net Terminalserver

Der ekey net Server kann UDP Informationen im sogenannten binären „RARE-Format" versenden.

19.2 UDP-Versand am ekey CV-LAN

Der ekey net CV LAN kann UDP Informationen im sogenannten „RARE-Format" versenden oder im neuen „net" Format, dieses wird als Klartext übertragen.

Dieser ist am ***ekey net CV LAN*** (ab Firmware 2.1.11.21) im Programm „ekey CONVERTER LAN config" aktivierbar.



19.3 UDP-Protokolle

Datenblockaufbau **„RARE"** vom Terminalserver oder vom ekey net CV LAN

Datenfeld Name	Anzahl in Byte	Datentyp	Werte-bereich	Bedeutung	
VERSION	4	long	3	Version der Daten	
Aktions Code	4	long	0000-9999	ActionCodeNone	0
				ActionCodeEnter	1
				ActionCodeLeave	2
				ActionCodeRefused	3
				ActionCodeUnknown	4
				ActionCodeAlarmDevOn	5
				ActionCodeAlarmDevOff	6
				ActionCodeAlarmLevel0	7
				ActionCodeAlarmLevel1	8
				ActionCodeAlarmLevel2	9
				ActionCodeAlarmLevel3	10

				ActionCodeUserMode0 11 ActionCodeUserMode1 12 ActionCodeUserMode2 13 ActionCodeUserMode3 14 ActionCodeReboot 15
Terminal ID	4	long	1-MAX_UINT	ID des Terminals
SERIENNR FS	14	String	xxxxxxx xxxxxxx	Stelle 1-6 = Artikelnummer Stelle 7-10 = Wochencode Stelle 11-14 = fortlaufende Nummer
Relais ID	1	String	0	Ist immer 0
Reserviert	1	String	0	Unbenutzt
Benutzer ID	4	long	0-MAX_UINT	ID des Benutzers
Finger ID	4	long	0-9	ID des Fingers
Ereignis	16	String	00000000 00000000	Ist immer leer
Zeit	16	String		Jjjjmmdd hhmmss
Name	2	Short	0	Name des users in Unicode, wenn vorhanden – leer *
Personal ID	2	Short	0	PersonalID – leer *

*=Diese Informationen kann nur der Terminalserver senden nicht der CV-LAN.



Datenblockaufbau **„net"** vom ekey net CV LAN

Datenfeld Name	Stellen-anzahl	Datentyp	Werte-bereich	Bedeutung
PAKETTYP	1	String	1	Pakettyp „Nutzdaten"
USER ID	6	String (dezimal)	0-999999	BenutzerID aus ekey net 000000: undefiniert
FINGER ID	1	String (dezimal)	0-9	1 = linker kleiner Finger 2 = linker Ringfinger . . 0 = rechter kleiner Finger ‚-'= kein Finger
SERIENNR FS	14	String	xxxxxxx xxxxxxx	Stelle 1-6 = Artikelnummer Stelle 7-10 = Wochencode Stelle 11-14 = fortlaufende Nummer „**************" – undefiniert
EREIGNIS	6	String	0-999999	EreignisID aus ekey net

Um den UDP-Paketversand zu prüfen, können Sie zb.: www.wireshark.org verwenden.

20 ekey net SDK

ekey net besitzt eine Softwareschnittstelle, die die Steuerung über fremde Anwendungen (Zeiterfassung usw.) erlaubt. Diese Schnittstelle ist im Rahmen dieses Handbuches nicht näher beschrieben. Für Informationen dazu nehmen Sie Kontakt mit ekey auf.

21 Wartung

21.1 Software

Trotz der Tatsache dass ekey net ein hochqualitatives Softwareprodukt ist, ist es doch nicht auszuschließen, das vereinzelt Fehlfunktionen vorkommen. Bitte melden Sie Fehler an den ekey Produktsupport. ekey veröffentlicht in definierten Zeitabständen (etwa 2 x pro Jahr) Neuversionen mit

- behobenen Fehlern
- meist neuen Features
- Verbesserungen der Performance.



Über neue Versionen von ekey net können Sie sich auch auf unserer Webseite www.ekey.net informieren.

21.2 Hardware

Grundsätzlich sind die Hardwareteile:

- ekey net FS
- ekey net SE
- ekey CVLAN
- ekey CV WIEG

keiner besonderen Wartung zu unterziehen.

Schäden

Wir empfehlen jedoch mindestens einmal pro Jahr alle Geräte einer optischen Inspektion zu unterziehen und

- defekte Gehäuse und Gehäuseteile
- eventuelle Kabelschäden
- usw.

zu erfassen und die Schäden zu beheben.

Verunreinigungen

Verunreinigungen am ekey net FS, speziell im Sensorbereich sind mit einem feuchten (nicht nassen!!!), nicht „kratzenden oder schleifenden" Tuch zu entfernen. Verwenden Sie dazu ausschließlich warmes Wasser ohne Putzmittel, Lösungsmittel usw.